Николай Николаевич ФЕДОТОВ –
выпускник Московского университета,
кандидат физ-мат. наук.

Автор книги профессионально занимается вопросами технической и правовой защиты информации на протяжении последних восьми лет. Он неоднократно участвовал в «компьютерных» делах в качестве специалиста или эксперта, опубликовал более десятка статей по соответствующей теме.

Обновления. Консультации

www.forensics.ru

БЕСПЛАТНО

ФОРЕНЗИКА – компьютерная криминалистика

Н. Н. ФЕДОТОВ

Николай Николаевич
ФЕДОТОВ

ФОРЕНЗИКА –
компьютерная криминастика

ИЗДАТЕЛЬСТВО
Юридический Мир

Николай Николаевич
ФЕДОТОВ

Форензика – компьютерная криминалистика

Издательство
«Юридический Мир»

Москва
2007

Федотов Н.Н. **Форензика – компьютерная криминалистика** – М.: Юридический Мир, 2007. – 432 с.

Фоpéнзика – прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании доказательств в виде компьютерной информации, методах поиска, получения и закрепления таких доказательств. Форензика является подразделом криминалистики.

Книга рассказывает о методах раскрытия и расследования компьютерных преступлений, правилах сбора, закрепления и представления доказательств по ним применительно к российскому законодательству. В книге имеются также сведения, относящиеся к гражданским делам, в которых затрагиваются информационные технологии, – таким как дела об авторских правах на программы для ЭВМ и иные произведения в электронной форме, дела о доменных именах, дела об использовании товарных знаков и других средств индивидуализации в Интернете.

Кто должен прочитать эту книгу:

- оперативные сотрудники правоохранительных органов;
- следователи;
- эксперты;
- судьи;
- государственные обвинители;
- адвокаты;
- студенты юридических специальностей;
- работники служб информационной безопасности;
- правозащитники.

Каждый из упомянутых категорий, прочитав книгу, сможет приобрести или усовершенствовать свои знания, касающиеся киберпреступлений.

В книге сделан упор на практику: описывается, как практически реализовать то или иное мероприятие, приведены примеры работы с цифровыми доказательствами из реальных уголовных и гражданских дел.

ISBN 5-91159-013-1 © Юридический Мир, 2007

Оглавление

Введение **11**
Название *11*
Другие разделы *11*
Ценз *12*
Предмет 12
Целостность *13*
Форензика и прогресс *14*
Задачи 15
Общенаучные методы 16
Специальные методы 19
Формы 19
Привлечение специалистов 21
Хакеры на службе? *22*
Вовлечение общественности 23
Общественные связи (пиар) *23*
Потерпевший *24*
Роль экспертно-криминалистических подразделений 25
Современное состояние 26
Специальные технические средства 28
Аппаратные средства *30*
Экспертные программы *30*
Наборы хэшей *31*
Архивирование *32*
Значение спецсредств *32*
Криминалистические информационные системы *33*
Этапы 34
Контрфорензика 35
Заключение 36

1. Компьютерные преступления **37**
Что такое «компьютерное преступление»? *37*
Избыточная криминализация *38*
Криминалистическая характеристика 39
Статистика *40*
Личность вероятного преступника *41*
Оперативность *47*

Приоритетность расследования 49
Онлайн-мошенничество 50
Способ 50
Обстановка 52
Преступник 53
Потерпевший 53
Следы 53
Клевета, оскорбления и экстремистские действия в Сети 54
Способ 54
Преступник 57
Обстановка 58
Следы 59
DoS-атаки 59
Способ 59
Преступник 60
Обстановка 61
Потерпевший 62
Следы 64
Дефейс 65
Способ 65
Преступник 67
Следы 67
Потерпевший 68
Вредоносные программы 68
Способ 68
Преступник 69
Звонилки (dialers) 72
Следы 73
Кардерство 74
Способы 74
Получение 75
Реализация 76
Скиминг 77
Использование интернет-казино 80
Фиктивные покупки 80
Реальный пластик 83
Белый пластик 84
Посреднические онлайн-сервисы 85
Почему мошенничество? 86

Мошенничество с трафиком 87
Нарушение авторских прав в офлайне 88
Способ 88
Преступник 89
Потерпевший 89
Следы 90
Политизированность 91
Нарушение авторских прав в Сети 92
Способ 92
Преступник 92
Потерпевший 93
Следы 94
Фишинг 94
Способ 94
Преступник 101
Потерпевший 101
Киберсквоттинг 102
Определение 102
Правовая оценка 103
Другое 105
Платежи через Интернет 105
Терроризм и кибервойна 108
Мошенничество в онлайновых играх 109
Использование RBL 111
Накрутка 115
Заключение к разделу 1 118

2. Оперативно-розыскные мероприятия 119
Взаимодействие 119
Перехват и исследование трафика 121
Значение 121
Пример 121
Организация перехвата 125
Шифрованный трафик 127
Исследование статистики трафика 131
Netflow 131
Пример 131
Другие данные о трафике 136
Анализ заголовков пакетов 137

Избирательный перехват *138*
Исследование логов веб-сервера 139
Значение логов *139*
Содержание *141*
Можно ли доверять логам? *142*
Исследование системных логов 142
Системные логи Windows *143*
Системные логи UNIX и Linux *144*
Системные логи IOS *144*
Исследование логов мейл-сервера и заголовков электронной почты 145
Как устроено *145*
Следы *146*
Примеры *147*
Можно ли доверять заголовкам? *154*
Формат сообщений *155*
Документирование прохождения сообщений *155*
Деревенский вариант *155*
Провинциальный вариант *156*
Столичный вариант *156*
Анонимные ремейлеры *156*
Установление принадлежности и расположения IP-адреса 158
Уникальность *158*
Регистраторы *159*
Установление принадлежности IP-адреса через whois-клиент *160*
Установление принадлежности IP-адреса через веб-форму *162*
Корректность *162*
Трассировка IP-адреса *162*
Неуловимый IP *167*
Пространство и время *168*
Документирование *169*
Физическое расположение *169*
Пример *170*
Прочее *171*
Установление принадлежности доменного имени 172
Изучение ответа *175*
Достоверность данных регистратора *177*
Анонимизация владельцев *177*
Документирование *178*
Принадлежность адреса электронной почты 180

Почтовый ящик *180*
Передача сообщений *180*
Достоверность *186*
Установление *186*
Примеры *187*
Кейлогеры 191
Аппаратные кейлогеры *191*
Программные кейлогеры *192*
Интернет-поиск как метод ОРД 192
Заключение к разделу 2 195

3. Следственные действия 196
Осмотр компьютера 196
Особенности *196*
Стандарты *197*
Лог-файлы, доказательная сила логов 198
Определение *198*
Примеры *198*
Лог как доказательство *202*
Цепочка доказательности *203*
Корректность генерирующей программы *203*
Примеры *204*
Неизменность при передаче *205*
Корректность логирующей программы *206*
Неизменность при хранении логов *206*
Корректность изъятия *206*
Неизменность после изъятия *208*
Корректность интерпретации *208*
Процедура приобщения логов *209*
Деревенский вариант *209*
Провинциальный вариант *209*
Столичный вариант *210*
Снятие копии диска *211*
Стерильность *212*
Тактика обыска 212
Принципы *213*
Общие правила изъятия компьютерной техники при обыске *213*
Особенности *215*
Ноутбук (лэптоп, переносной компьютер) *216*

Наладонный компьютер (КПК) 216
Принтеры 217
Сканеры 218
Флэш-накопители 218
Мобильные телефоны 220
Коммутаторы и маршрутизаторы 220
Автомобильные компьютеры 221
Модемы 221
Цифровые фотоаппараты 222
Сменные накопители 222
Короткоживущие данные....................223
Перечень 223
Снятие 225
Как выключать?....................227
Работа с потерпевшими 229
Заключение к разделу 3 230

4. Заверение контента 231
Размещение на веб-сайте 232
Практика 232
Просмотр 233
Динамические веб-страницы 233
Особенности браузера....................234
Адресация 235
Размещение в телеконференции (newsgroup) 237
Размещение в файлообменных сетях 240
Доказательство наличия контента....................243
Выявление источника 244
Доказательство использования 244
Виды преступлений....................245
Контент и доменное имя 246
Правовая защита домена 246
Путаница сайта и ДИ 246
Примеры 247
Заключение к разделу 4 249

5. Компьютерно-техническая экспертиза 250
Место и роль КТЭ 250
Общее 250
Кто может быть экспертом? 251
Проблемы с пониманием 253
Приемлемые вопросы 254
Поиск информации 255
Следы 256
Программы 256
Время 257
Пользователь 257
Итоги 258
Неприемлемые вопросы....................258
Контрафактность 258
Стоимость 259
Правомерность доступа 260
Оценка содержания 261
Резюме 262
Объекты исследования....................263
Оригинал или копия?....................263
Методы КТЭ 264
Исследование файловых систем 264
Копирование носителей 267
Хэш-функции для удостоверения тождественности 269
Исследование файлов 271
Другие типы носителей 272
Флэш-накопители 272
Зашифрованные данные 274
Использование слабой криптографии 274
Использование коротких ключей и паролей 274
Использование словарных паролей 275
Неаккуратное обращение с открытым текстом 275
Неаккуратное обращение с паролем 276
Нешифрованные имена файлов 276
Ректотермальный криптоанализ....................277
Доступ к содержимому ОЗУ....................277
Использование кейлогера 277
Шифрование разделов и носителей....................278
Стеганография 278
Средства и инструменты 279
Экспертные инструменты и авторское право 279
Поиск информации на диске....................280

Информация о файлах...280
Подключение образа диска...282
Изучение архивов электронной почты и ICQ...282
Реконструкция просмотра веб-страниц...283
Оценка найденного...284
Исследование программ...286
Изучение печатных документов...287
Стоимость ПО...287
Разбор образцов...290
Отрицательный пример...290
Промежуточный пример...307
Положительный пример...311

6. Участие специалиста в судебном заседании...321

7. Тенденции и перспективы...323
Тенденции...323
Понимание и просвещение...324
Широкополосный доступ...325
Интеллектуальная собственность...326
Конвергенция...327
Перспективы...328
Законодательство...328
Криминалистическая техника...328
Слежка...328
Новые отношения...329
Неолиберализм и неоконсерватизм...330
Возрастание роли Интернета...331

Литература...332
Офлайновые публикации...332
Интернет-публикации...336
Нормативные акты...339

Официоз или сленг? Словарь официальных и жаргонных технических терминов...340

Введение

Название

Термин «форéнзика» произошел от латинского «foren», что значит «речь перед форумом», то есть выступление перед судом, судебные дебаты – это был один из любимых жанров в Древнем Риме, известный, в частности, по работам Цицерона. В русский язык это слово пришло из английского. Термин «forensics» является сокращенной формой «forensic science», дословно «судебная наука», то есть наука об исследовании доказательств – именно то, что в русском именуется криминалистикой. Соответственно, раздел криминалистики, изучающий компьютерные доказательства, называется по-английски «computer forensics». При заимствовании слово сузило свое значение. Русское «форензика» означает не всякую криминалистику, а именно компьютерную.

Другие разделы

Традиционные разделы криминалистики – дактилоскопия, баллистика, токсикология – развиваются уже более ста лет. В них не только накоплен большой опыт и отточены методики исследования. Некоторые особенности криминалистических технологий отражены в законодательстве. Например, законодательством прямо предусматривается взятие отпечатков пальцев и отстрел оружия в определенных случаях. Компьютерная криминалистика только что родилась. Опыт и инструментарий ее пока невелик. А требования законодательства совсем не заточены под особенности применяемых технологий, и даже иногда препятствуют их использованию.

Форензика оказалась почти не связанной с другими разделами криминалистики. Разве что прослеживается некоторая связь с технико-криминалистическим исследованием документов – компьютеры и компьютерная периферия широко применяются для подделки традиционных, бумажных документов.

Внутри форензики уже наметился один обособленный раздел – исследование программ для ЭВМ. Изучение устройства программ по исполняемому коду, методы создания вредоносных программ и противодействия им – это требует своих методов, существенно отличающихся от прочих методов форензики, применяемых для поиска, сбора и исследования цифровых доказательств. Хорошие специалисты по вредоносным программам, как правило, имеют узкую специализацию и не занимаются ничем иным – ни восстановлением скрытой информации, ни фиксацией короткоживущих данных, ни трассировкой источника DoS-атаки. И нап-

ротив, эксперт, специализирующийся на исследовании информационного содержимого компьютеров, вряд ли возьмется за исследование неизвестного компьютерного вируса.

Некоторые авторы разделяют компьютерную криминалистику (computer forensics) и сетевую криминалистику (network forensics). Применяемые методы в том и в другом случае действительно отличаются.

Ценз

Для полного понимания данной книги необходимо владеть компьютером на уровне продвинутого пользователя и иметь базисные представления о современных коммуникационных технологиях и Интернете.

Автор весьма опечален, что пришлось ограничить таким образом круг читателей, но, к большому сожалению, по-другому поступить невозможно. Понимание материала настоятельно требует специальных познаний.

Если вдаваться в подробные объяснения о том, что такое файловая система, как работает протокол TCP или почему мощность процессора не влияет на скорость интернет-соединения, то вместо работы по криминалистике получится пятисотстраничный самоучитель по работе на компьютере, в котором всего несколько страниц – по делу. Именно такая история происходит с большинство книг, изданных в Европе и США [1-6, 74], которым подошло бы название «Компьютерная криминалистика для чайников». Также практикуется чисто популяризаторский подход, при котором материал излагается поверхностно, хотя и занимательно; специальных знаний не требует, но и не дает [39].

Если в подробные объяснения не вдаваться, а просто привести определения всех используемых терминов, как это любят делать отечественные авторы, то подготовленный читатель будет на этих страницах скучать, а неподготовленный все равно ничего не поймет. Определения – не объяснения. Подобный метод изложения незнакомого материала напоминает книгу на иностранном языке, к которой приложен словарь этого языка; одним читателям он не нужен, другим не поможет.

Поэтому не остается ничего иного, как рассчитывать на определенный уровень компьютерной грамотности читателя.

А имеющийся в конце книги словарь компьютерных терминов преследует совсем иную цель – отделить устоявшиеся термины от жаргонных и указать, какие из многочисленных вариантов следует использовать в официальных документах.

Предмет

Форензика (компьютерная криминалистика) является прикладной наукой о раскрытии и расследовании преступлений, связанных с компьютерной информацией, о методах получения и исследования доказательств, имеющих форму компьютерной информации (так называемых цифровых доказательств), о применяемых для этого технических средствах.

Предметами форензики являются:

- криминальная практика – способы, инструменты совершения соответствующих преступлений, их последствия, оставляемые следы, личность преступника;
- оперативная, следственная и судебная практика по компьютерным преступлениям;
- методы экспертного исследования компьютерной информации и, в частности, программ для ЭВМ;
- достижения отраслей связи и информационных технологий (ИТ), их влияние на общество, а также возможности их использования как для совершения преступлений, так и для их предотвращения и раскрытия.

Целостность

Несколько слов об особенностях изучаемых следов. Почти все следы, с которыми приходится работать специалисту по форензике, имеют вид компьютерной информации, регулярной или побочной. Их достаточно легко уничтожить – как умышленно, так и случайно. Часто их легко подделать, ибо «поддельный» байт ничем не отличается от «подлинного». Фальсификация электронных (цифровых) доказательств выявляется либо по смысловому содержанию информации, либо по оставленным в иных местах следам, тоже информационным. Цифровые доказательства нельзя воспринять непосредственно органами чувств человека, но только через посредство сложных аппаратно-программных средств. Поэтому эти следы сложно продемонстрировать другим лицам – понятым, прокурору, судье. Не всегда просто обеспечить неизменность следов при их хранении. И не только обеспечить, но и доказать суду эту неизменность.

Вообще, понятие «неизменность» лишь с натяжкой применима к компьютерной информации. На некоторых видах носителей она хранится действительно статически – в виде разной намагниченности участков носителя или вариаций его оптических свойств. Но в других случаях метод хранения информации таков, что предусматривает постоянную смену носителя. Или предусматривает случайные величины.

Оперативная память компьютера (типа DRAM) регенерируется раз в несколько миллисекунд. То есть записанные там сигналы фактически стираются и записываются вновь. При передаче по многим каналам связи используется помехоустойчивое кодирование в расчете на возникающие при передаче ошибки; эти ошибки неизбежно возникают, но исправляются на принимающей стороне линии за счет избыточности кода. В

центральном процессоре тоже постоянно происходят ошибки при совершении арифметическо-логических операций, но если их не слишком много, они исправляются благодаря внутренней диагностике. В сетевых протоколах, которые мы считаем «надежными», таких как TCP, эта надежность достигнута именно за счет того, что пропавшие в пути датаграммы или иные блоки информации переписываются, пока не будет подтвержден их верный прием. Запись на компакт-диск ведется с использованием кода Рида-Соломона с коррекцией массовых ошибок. То есть технология заведомо рассчитана на возникновение ошибок на этапе считывания. И такие ошибки всегда возникают. Но исправляются благодаря избыточности кода. Одним словом, «неизменной» компьютерную информацию может воображать лишь пользователь, который не знает подробностей внутреннего устройства компьютерной техники и программного обеспечения.

Специалисты говорят про «неизменность» только с такими пользователями. Между собой они используют понятие «целостность», подразумевая, что информация может в процессе хранения и передачи сколько угодно раз изменяться, перекодироваться или сменять носители. Требуется лишь, чтобы первоначальная информация совпадала с конечной с точностью до одного бита – это и есть целостность.

Форензика и прогресс

Теперь – о технических достижениях. Влияние передовых достижений техники и технологии на преступность возможно тремя путями.

Во-первых, неостановимый технический прогресс дает возможность совершать преступления новыми способами и при помощи новых орудий. Естественно, в той же мере прогресс способствует появлению новых способов раскрытия преступлений – как старых, так и новых. Например, то же старое мошенничество в наш век совершается при помощи сети Интернет. Но суть и предмет посягательства у мошенничества прежние. Новыми являются лишь орудия совершения – веб-сайт, электронная почта, платежная система.

Во-вторых, достижения информационных технологий порождают принципиально новые общественные отношения, каковые отношения и становятся предметом преступных посягательств. При этом способ посягательства и орудия могут быть как старыми, так и новыми, с учетом достижений ИТ. Самый яркий пример – доменные имена. Такого общественного отношения, как право распоряжаться доменным именем, до недавних пор просто не существовало. Не было и посягательств. Ныне доменные имена охраняются законом (они причислены к объектам интеллектуальной собственности). И существует целый класс правонарушений, связанных с доменами, – киберсквоттинг*.

В-третьих, развитие ИТ может привести к появлению не просто новых общественных отношений, но нового субъекта таких отношений. Появление полноценного искусственного интеллекта уже явно просматривается на научном горизонте. А пока можно говорить о первых шагах в этом направлении. Программа для ЭВМ еще не рассматривается в качестве субъекта права, но в качестве стихийной силы уже иногда рассматривается. Программам уже дано принимать решения, которые могут существенно влиять на благосостояние и даже жизнь людей. Программы уже могут порождать новые объекты авторского права. Словом, появление принципиально нового субъекта, нового члена общества со своими правами – искусственного интеллекта – не за горами. А его появление вызовет новые правоотношения и, соответственно, новые преступления.

Задачи и приложения

Форензика решает следующие задачи:

- разработка тактики оперативно-розыскных мероприятий (ОРМ) и следственных действий, связанных с компьютерной информацией;
- создание методов, аппаратных и программных инструментов для сбора и исследования доказательств компьютерных преступлений;
- установление криминалистических характеристик правонарушений, связанных с компьютерной информацией.

Сферы применения форензики суть следующие.

1. Раскрытие и расследование уголовных преступлений, в которых фигурируют компьютерная информация как объект посягательства, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства.
2. Сбор и исследование доказательств для гражданских дел, когда такие доказательства имеют вид компьютерной информации. Особенно это актуально по делам о нарушении прав интеллектуальной собственности, когда объект этих прав представлен в виде компьютерной информации – программа для ЭВМ, иное произведение в цифровой форме, товарный знак в сети Интернет, доменное имя и т.п.
3. Страховые расследования, проводимые страховыми компаниями касательно возможных нарушений условий договора, страхового мошенничества, особенно когда объект страхования представлен в виде компьютерной информации или таким объектом является информационная система.
4. Внутрикорпоративные расследования инцидентов безопасности, касающихся информационных систем, а также работы по предотвращению утечки информации, содержащей коммерческую тайну и иные конфиденциальные данные.

5. Военные и разведывательные задачи по поиску, уничтожению и восстановлению компьютерной информации в ходе оказания воздействия на информационные системы противника и защиты своих систем.
6. Задачи по защите гражданами своей личной информации в электронном виде, самозащиты своих прав, когда это связано с электронными документами и информационными системами [5, W16].

Во многих из этих приложений некоторые методы форензики очень тесно интегрированы с методами технической защиты информации. Эти методы даже кое-где пересекаются. Несмотря на это, форензика никак не может быть приравнена к защите информации, поскольку цели у этих дисциплин разные.

Общенаучные методы

Все научные методы (наблюдение, измерение, описание, сравнение, эксперимент, моделирование, объяснение, анализ, синтез, предсказание) применяются в компьютерной криминалистике без ограничений. Хотя имеют некоторые особенности.

Такой общенаучный метод, как наблюдение, применяется в форензике достаточно своеобразно. Дело в том, что основным объектом исследования является компьютерная информация, которая в принципе не может наблюдаться человеком непосредственно. И изменяться непосредственно также не может. Непосредственные органы чувств человека – зрение, слух, осязание – не в состоянии воспринимать компьютерную информацию. Но это еще не настоящее своеобразие. В мире много объектов, которые не могут восприниматься человеком непосредственно – глазами, ушами и пальцами. Это еще не повод объявлять соответствующую науку уникальной. Для наблюдения «ненаблюдаемых» величин есть большое количество инструментов и способов – микроскопы, вольтметры, интерферометры и так далее. При помощи таких инструментов-посредников человек может наблюдать и изучать то, что не наблюдается невооруженным глазом. Все дело в сложности, детерминированности и прозрачности принципов действия таких «технических посредников».

При изучении компьютерной информации количество и сложность таких посредников настолько велики, что количество это переходит в качество. Мы не всегда знаем всех посредников, стоящих между информацией на компьютерном носителе и нашими глазами. Мы с большим трудом можем представить, какие именно преобразования претерпела информация по пути от своей исходной формы до наших глаз.

Представим себе, что на месте преступления обнаружен след – отпечаток обуви. Он воспринимается органами чувств человека непосред-

ственно. Если для восприятия и требуются какие-то технические средства, то лишь самые простые (например, фонарик или очки), принцип действия которых ясен любому и легко представим. А чаще технических средств и вовсе не требуется. Следователь и понятые своими глазами видят отпечаток обуви, прекрасно понимают механизм его возникновения. Не испытывая сомнений, они фиксируют этот след в протоколе, а после готовы показать под присягой, что видели именно отпечаток обуви. И у судьи не появится сомнений, что они могли видеть не то, что было на самом деле.

Совсем по-другому с компьютерной информацией.

Представим, что на «месте происшествия», а именно на диске сервера, в лог-файле*[1] обнаружена запись. Органами чувств человека она не воспринимается. Чтобы увидеть эту запись, потребуется посредничество следующих технических средств:

- механизм жесткого диска (НЖМД*);
- контроллер НЖМД с внутренней микропрограммой (firmware);
- внешний ATA-контроллер;
- программное обеспечение BIOS;
- операционная система;
- файловая система (драйвер);
- программное обеспечение для просмотра содержимого файла (например, вьювер «`less`»);
- драйвер экрана;
- программный экранный шрифт;
- аппаратные средства ввода и вывода (клавиатура, монитор) со своими собственными микропрограммами.

Вот сколько посредников стоят между компьютерной информацией и глазами «очевидца»! Все они изготовлены разными производителями. Не для всех из них имеются единые технические стандарты. Не для всех доступны описания. И ни в одном из этих средств нельзя быть полностью уверенным – все знают об ошибках в программном обеспечении, о возможности вирусов, троянов* и программных закладок. Могут ли понятые уверенно утверждать, что именно они видели? Даже не рассматривая возможности намеренных закладок в программах... А если оператор, запуская вьювер, ошибся на одну букву в имени каталога или файла? А если «`/var`» – это не локальный диск, а подмонтированный сетевой? А если владелец аккаунта* сделал себе удобства ради такой, например, алиас:

```
alias less='grep -v "Deny UDP"
```

[1] Звездочкой отмечены термины, которые имеются в прилагаемом словаре.

то что же мы увидим, думая, что просматриваем лог-файл командой «`less /var/log/security.log`»? Мы увидим вместо настоящего лог-файла картину, мягко выражаясь, сильно искаженную, а лучше сказать – вовсе неверную.

Итак, особенностью наблюдения в отношении компьютерной информации является то, что непосредственно наблюдаемое (то есть изображение на экране монитора) имеет отношение к объекту наблюдения (то есть компьютерной информации) не просто косвенное, а очень-очень-отдаленно-посредственно-седьмая-вода-на-киселе-косвенное отношение. По пути происходит не просто большое количество преобразований, но непредставимо большое, трудно контролируемое, зависящее от множества незнакомых людей и невоспроизводимых факторов количество преобразований.

Другие общенаучные методы – анализ и синтез – также имеют в обсуждаемой науке свои особенности.

Дело в том, что в других технических науках при изучении объектов мы имеем дело только с объективными физическими процессами. Здесь же мы сталкивается со свободной человеческой волей, которая «зашита» в такой объект исследования, как программа для ЭВМ. Будучи объектом искусственного происхождения, программа несёт в себе волю программиста, отпечаток его личности, выполняет его замыслы, реализует его видение. То есть программа для ЭВМ – это уже не в полной мере объективная реальность. Хотя до полноценного субъекта – искусственного интеллекта – ей еще далеко.

Поясним утверждение на примере. Известно, что злоумышленник мог установить на свой компьютер программу типа «логическая бомба*» для уничтожения всей критичной информации при угрозе попадания компьютера в чужие руки. Она должна сработать при заданных условиях: при выполнении каких-то действий на компьютере или, наоборот, – при невыполнении каких-то действий. Оставим сейчас за скобками стандартный метод (отключение компьютера, изъятие из него носителя информации и изучение его копии, что делает невозможным активацию программы-бомбы) и зададимся вопросом: как можно определить условия срабатывания такой программы для ее нейтрализации? Подумав немного, приходим к выводу, что ключ к пониманию алгоритма действия и условий срабатывания сей неизвестной программы следует искать исключительно в голове ее автора. Только поняв его образ мыслей и шаблоны поведения, можно догадаться, как поведет себя его программа. Формально программа – детерминированный объект. Но фактически изучать ее надо через изучение субъекта, обладающего свободой воли. То есть программа как бы обладает свободой воли, во всяком случае, такое допущение откроет нам путь к ее познанию.

Но разве не возникает та же ситуация с иными техническими устройствами, включая механические? Разве на их работу не наложила отпечаток личность создателя? Автор берётся утверждать, что вышеописанная особенность характерна лишь для устройств, реализующих довольно сложный алгоритм. Алгоритм – это как раз тот объект, в котором и может содержаться частичка «воли». Кроме компьютерных программ, какие устройства реализуют алгоритмы? Причем алгоритмы не примитивные, а достаточно сложные, многовариантные. Теоретически такие устройства могут существовать, но в своей жизни автор их не встречал. Поэтому он берется утверждать, что только компьютерные программы обладают описанным свойством, то есть могут рассматриваться как обладающие условной свободой воли.

Специальные методы

Наряду с общенаучными форензика применяет и специальные методы исследования, свойственные только ей. Назовем некоторые из этих методов.

- Создание и применение специализированных криминалистических информационных систем; перенастройка и использование в своих целях систем двойного назначения.
- Использование в целях обнаружения или исследования доказательств публичных поисковых систем (таких как «Google»), а также поисковых систем специального назначения (типа «Эшелон»).
- Создание виртуальной личности для целей проведения с ее помощью ОРМ и агентурной работы.
- Сбор хэш-функций известных файлов для отделения их от файлов, содержащих оригинальную пользовательскую или модифицированную информацию.
- Архивирование полного содержимого носителей для целей последующего расследования возможных инцидентов.
- Эмулирование сетевых сервисов для исследования поведения подозрительных программ в лабораторных условиях.

Формы

Общенаучные и специальные методы компьютерной криминалистики должны использоваться в борьбе с преступностью в следующих формах.

1. Производство компьютерно-технических экспертиз. Кроме этих, «родных» для себя экспертиз, ИТ-специалисты должны принимать участие в некоторых других видах экспертиз. Например, товароведческая

(экономическая) экспертиза по определению стоимости прав на использование экземпляра ПО. Такая экспертиза совершенно необходима для доказывания нарушения авторских прав (ч.ч. 2 и 3 ст. 146 УК), где квалифицирующим признаком является стоимость контрафактных экземпляров или прав на использование произведения. Понятно, что обычный экономист не знаком с особенностями ценообразования на программные продукты, с существующей практикой в этой области. Поэтому ему надо дать в помощь эксперта по ИТ.

2. Участие специалистов в проведении следственных действий, имеющих отношение к компьютерной информации, – обыска, выемки, осмотра места происшествия и т.д. Например, такая элементарная задача, как выключение компьютера, который подлежит изъятию. Нет однозначного способа выключения. Чтобы правильно его выключить, нужно проанализировать обстоятельства дела, взвесить вероятности разных событий и, только исходя из этого, избрать способ выключения. А некоторые типы компьютерной техники вообще выключать нельзя.

3. Участие специалиста в проведении ОРМ. Наиболее востребованное в обсуждаемой области мероприятие – снятие информации с технических каналов связи – проводится не просто «при участии», а только самим специалистом.

4. Участие специалиста в судебном заседании. Эта форма, предусмотренная УПК, стала активно использоваться лишь при рассмотрении дел по компьютерным преступлениям. В таких делах специальные знания требуются очень часто. Без разъяснений специалиста иногда невозможно правильно понять не только заключение эксперта, но также показания свидетелей, имеющиеся в деле справки, вопросы участников процесса. Специалист в зале суда может действовать наподобие переводчика, разъясняя участникам процесса значения терминов, поясняя значение тех или иных технических деталей и так далее.

5. Снабжение оперативных работников и следователей техническими средствами, которые те могут использовать в работе самостоятельно, без участия специалиста.

6. Обучение пользователей и технических специалистов предприятий (то есть потенциальных потерпевших) методам первичной фиксации цифровых доказательств, их предохранения от уничтожения. Значительная часть компьютерных преступлений остается нераскрытой только из-за того, что оператор информационной системы, которая стала целью злоумышленника, не позаботился о сбережении логов*, электронных сообщений, использованных программ и иных потенциальных доказательств. Либо не знал, как их правильно сберечь, чтобы в дальнейшем такие доказательства имели силу, либо вообще не подозревал о существовании некоторых цифровых следов.

Привлечение специалистов

Специалист или эксперт должен привлекаться к расследованию или проведению ОРМ в тех случаях, когда требуются специальные знания («специальные познания» в терминологии предыдущей редакции УПК) в какой-либо области.

Несмотря на повсеместное распространение компьютерной техники, знания об этой технике не распространяются вслед за ней, столь же повсеместно.

Современная парадигма ИТ предусматривает отчуждение пользователя от управления работой ЭВМ. Развитие идет в направлении всё большего и большего абстрагирования пользовательского интерфейса от процессов в компьютере. Пользователь 1960-х и 1970-х годов мыслил байтами и логическими операциями. Пользователь 1980-х – символами и файлами. Пользователь 1990-х – окнами, «папками» и событиями. В текущем десятилетии типичный пользователь думает такими объектами, как «документ» и «рабочий стол». То есть для идеального пользователя никаких специальных знаний о внутренних процессах в вычислительной технике не требуется.

Криминалистическое же исследование предполагает как раз глубокое проникновение в суть процессов, происходящих в ЭВМ и компьютерных сетях. Чем глубже погружается исследователь в подробности функционирования, тем больше он обнаруживает следов действий пользователя.

К примеру, оценивая следы при просмотре пользователем веб-сайта, неспециалист (скажем, следователь) может заключить, что следы (доказательства) следует искать в двух местах – на персональном компьютере пользователя и на сервере, на котором расположен веб-сайт. И это будет ошибкой. Не обладая знаниями, глубже определенного, положенного для пользователя уровня, следователь упускает из виду обращение к DNS-резолверу пользователя, а также рекурсивные обращения этого резолвера к нескольким DNS-серверам. Такие обращения могут логироваться и служить полноценными (то есть не косвенными, не дополнительными, а вполне самостоятельными) доказательствами посещения определенной веб-страницы. Еще десяток видов следов при таком простом действии, как просмотр веб-страницы, перечислен в главе «Исследование логов веб-сервера» раздела 2.

Автор полагает, что при любых ОРМ или следственных действиях, связанных с компьютерной информацией, привлечение специалиста обязательно. Ибо специальные знания в сфере ИТ позволяют видеть неочевидное, находить бесследно пропавшее и обманывать безошибочное. И попутно еще опровергать все утверждения из «инструкции для пользователя», ибо обычный среднеквалифицированный пользователь работает

с компьютером на определенном, предназначенном для него уровне, а всё, что глубже, ему знать «не положено».

Хакеры на службе?

Отдельного разговора заслуживает тема привлечения киберпреступников для противодействия другим киберпреступникам – в качестве работников служб информационной безопасности или даже сотрудников правоохранительных органов.

Тот, кто совершает преступления, конечно же, хорошо представляет себе методы их совершения, лучше видит возможности, уязвимости, знает психологию киберпреступников, ориентируется на черном рынке соответствующих услуг. Этим он ценен для борьбы с преступностью, своими знаниями.

Но знания – дело наживное. Обучить соответствующей специальности можно почти любого человека, особенных способностей тут не требуется.

Кроме знаний киберпреступник отличается также специфическими наклонностями. В их число входит неприятие многих социальных институтов, пренебрежение интересами иных лиц и общества в целом. Иногда также патологическая склонность к антисоциальному поведению [W27]. Если знаниям можно обучить, то подобным наклонностям невозможно «разучить» человека. Именно поэтому нигде в мире на службу в правоохранительные органы не берут преступников, даже бывших (во всяком случае, автору такая практика не известна). Их используют в качестве агентов или консультантов, но не более.

Французская уголовная полиция «Сюртэ» считается самой первой в мире службой уголовного розыска. Ее основатель и первый руководитель, Эжен-Франсуа Видок был многократно судимым профессиональным вором. И первый штат, который он набрал, также целиком состоял из бывших профессиональных преступников [68]. Результаты работы подразделения Видока впечатляли. Такой статистикой раскрытых преступлений, как у него (811 раскрытых преступлений в год на 12 человек), не могла похвастаться ни одна спецслужба ни в XIX, ни в XX веке. Это, пожалуй, единственный удачный пример привлечения бывших уголовников на правоохранительную службу. Для всех последующих политических и государственных деятелей лояльность полиции была несравненно важней ее эффективности. Впрочем, и эффективность службы бывших преступников также иногда ставится под сомнение.

Автор также в свое время отдал должное этой идее. Но результаты поиска возможностей привлечения хакеров к деятельности по защите информации оказались неудовлетворительными. Оказалось, что среди киберпреступников попросту нет достаточно квалифицированных кадров.

Зарплата рядового сисадмина в Москве в 1999 году была в разы выше, чем средний доход спамера*, вирусописателя или интернет-мошенника. (Правда, с кардерами* ситуация была иная, но для этой криминальной профессии особые технические навыки и не требуются.) Иными словами, много выгоднее быть законопослушным. С тех пор ситуация изменилась. Количество денег и иных материальных интересов в Интернете (в частности, в российском его сегменте) сильно возросло. Ныне ремесло киберпреступника уже в состоянии прокормить хорошего специалиста. Правда, и средние доходы честного онлайнового бизнесмена также выросли.

Тем не менее автор согласен с общепринятым мнением, что привлекать киберпреступников для борьбы с киберпреступностью допустимо лишь в качестве осведомителей, в крайнем случае – консультантов.

Вовлечение общественности

Да не смутит читателя этот заголовок, созвучный с пустыми пропагандистскими заклинаниями советских времен. Речь пойдет о совсем другом вовлечении другой общественности.

Для расследования компьютерных преступлений необходимо сотрудничество со стороны потерпевшего, а также со стороны свидетелей. Необходимо как-то узнать о самом факте совершения преступления. В ряде случаев необходимо получить официальное заявление от потерпевшего.

Свидетели и потерпевшие для компьютерных преступлений – это чаще всего пользователи ЭВМ и профессиональные ИТ-специалисты. Потерпевшим также часто являются предприятия, от лица которых принимают решения те же ИТ-специалисты. Но среди данной категории граждан не принято обращаться в правоохранительные органы по поводу инцидентов безопасности. И, напротив, при обращении органов к ним они не склонны сразу идти на сотрудничество, стараются уклониться от дачи показаний и не ожидают ничего хорошего от такого взаимодействия.

Статистика опросов говорит нам, что до 80% инцидентов безопасности попросту скрывается сотрудниками даже от своего начальства, не говоря уже о правоохранительных органах.

Общественные связи (пиар)

Полезность общественных связей для раскрытия, расследования, а также предупреждения преступлений уже никем не ставится под сомнение. В отношении компьютерных преступлений такое утверждение также справедливо. Особенность в том, что аудитория традиционных СМИ не вполне соответствует интересующей нас специфической группе – корпоративные ИТ-специалисты, ведущие бизнес в Интернете предпринима-

тели и простые пользователи персональных компьютеров. Для эффективного взаимодействия с этой аудиторией целесообразно использовать иные средства – сетевые СМИ, блоги, интернет-рекламу.

В газетах и телепередачах довольно часто рассказывается о совершенных и раскрытых преступлениях. Эти публикации вызывают интерес читателей и зрителей. Пользуясь таким интересом, правоохранительные органы проводят собственные пиар-мероприятия. Но когда в специфических онлайновых* СМИ публикуется сообщение о каком-либо компьютерном преступлении или интервью с представителем правоохранительных органов на тему киберпреступности, реакция аудитории бывает и негативной. Автор изучил десятки подобных публикаций с комментариями на них. Положительных и нейтральных отзывов – ничтожное количество. Большинство комментариев либо ругательные, либо ехидные, либо указывающие на некомпетентность источника в том или ином техническом вопросе. Совершенно очевидно, что пиар-стратегия для онлайновых СМИ в отношении компьютерных преступлений должна быть иной, не такой же, как для традиционных СМИ в отношении традиционных преступлений. Специфика аудитории (высокая квалификация в технических вопросах) и специфика способа коммуникации (моментальные комментарии) требуют особого подхода.

Потерпевший

Во многих случаях для расследования компьютерного преступления бывает очень полезно привлечь потерпевшего.

Классическая виктимология не склонна была рассматривать потерпевшего как опору следствия и источник существенной помощи (за исключением предоставления информации). Современная виктимология сменила точку зрения [62, 63]. Жертва преступления, оказывается, имеет хороший потенциал и мотивацию для активных действий. Следствию было бы неразумно не использовать эти возможности. В рамках закона, естественно. Ныне зарубежные криминологи рекомендуют привлекать потерпевшего к активным действиям по расследованию как данного, так и других аналогичных преступлений.

Сказанное выше касается традиционных, не компьютерных преступлений. А в нашем случае полезность потерпевшего может быть еще выше. Для неправомерного доступа к компьютерной информации, корпоративного мошенничества, кардерства и некоторых других высокотехнологичных видов преступлений потерпевшие (или работники предприятия-потерпевшего) имеют достаточно высокую квалификацию в области ИТ. Часто эта квалификация выше, чем у сотрудников правоохранительных органов, которые занимаются расследованием. Кроме квалификации есть и мотивация.

Автор неоднократно сталкивался с ситуацией, когда руководитель фирмы, пострадавшей от действий кардера*, ассигновал значительные средства, чтобы содействовать привлечению виновного к ответственности. Вовсе не потому, что надеялся получить с осужденного преступника компенсацию причиненного ущерба. Это далеко не главный мотив. Оправдаться перед клиентами, которые доверили свои персональные данные, перед акционерами, перед партнерами, компенсировать ущерб деловой репутации фирмы. Предотвратить возможные рецидивы или месть злоумышленника, который остался безнаказанным. Всё это заставляет потерпевшее предприятие предлагать свою помощь следствию – информацией, техникой, специалистами, разными услугами.

Физические лица, оказывавшиеся потерпевшими, также склонны содействовать обнаружению преступника. Автору неоднократно приходилось уговаривать пострадавших ИТ-специалистов отказаться от самостоятельного поиска и наказания преступника, чем они намеревались заняться, не веря в возможности правоохранительных органов или просто не вспоминая об их существовании. Бывали случаи, когда такой специалист не просто оказывал помощь милиции, а фактически преподносил им на блюдечке раскрытое преступление.

Роль экспертно-криминалистических подразделений

Как можно понять из главы «Привлечение специалистов», роль специалистов и экспертов при раскрытии и расследовании компьютерных преступлений является ключевой. Без их участия расследовать такое преступление невозможно вообще.

Особенность состоит в том, что экспертно-криминалистические подразделения правоохранительных органов таких специалистов не имеют. В текущих условиях минимальная зарплата ИТ специалиста «на гражданке» в разы превышает максимальную зарплату сотрудника экспертно-криминалистического подразделения в органах внутренних дел, юстиции или ФСБ. Старых же кадров, на которых держатся другие направления криминалистики, для форензики попросту не существует, поскольку обсуждаемая отрасль знания сама по себе очень молода.

Номинальное существование подразделений компьютерно-технической экспертизы в некоторых ЭКУ может ввести кого-то в заблуждение, но только до первой встречи с этими номинальными «экспертами» или их трудами.

Выход состоит в привлечении к расследованию гражданских специалистов и экспертов из числа сотрудников операторов связи, программистов, инженеров по коммуникационному оборудованию, системных администраторов. Многие из них готовы сотрудничать с органами внутрен-

них дел совсем безвозмездно или за... скажем так, на иных взаимно приемлемых условиях.

Нечто вроде экспертно-криминалистических отделов существует в некоторых коммерческих организациях, которым часто приходится проводить расследования инцидентов безопасности или которые специализируются на проведении экспертиз по гражданским делам.

Штатным же ЭКО стоит поручать лишь простейшие, типовые виды компьютерных экспертиз, для которых есть готовые алгоритмы действий и образцы заключений.

Современное состояние

В развитых странах форензика как прикладная наука существует полноценно: издан ряд научных трудов, имеются кафедры и учебные курсы, практические работники при раскрытии компьютерных преступлений обязаны следовать официальным рекомендациям, написанным соответствующими специалистами [7].

В прочих (не относящихся к развитым) странах форензика находится пока в зачаточном состоянии. Россия принадлежит к числу таковых. В то же время качественные характеристики российских компьютерных специалистов находятся на передовом уровне, не уступая развитым странам. Особенности советской системы высшего образования, особенно ее исследовательский уклон в подготовке кадров, привели к тому, что российские специалисты отличаются от западных креативностью, способностью быстро осваивать новые знания, критичностью мышления – это как раз то, что требуется для успешного совершения компьютерных преступлений и их раскрытия.

Однако привлечение таких специалистов на службу в правоохранительные органы или на работу в научные криминалистические учреждения сильно затруднено. Во-первых, уже упоминавшаяся низкая оплата по сравнению с ИТ-компаниями. Во-вторых, в какой-то мере естественная инертность научных кругов и медленная смена поколений в научной и ведомственной иерархии. Все это не позволяет новым специалистам влиться в криминалистическую науку, а уже существующие работники не в состоянии переквалифицироваться.

Характерный пример. Некоторое время назад знакомый автора уволился из органов внутренних дел, где он служил оперуполномоченным в управлении «К» (ранее – УБПСВТ) одного из субъектов Федерации. Он давно уже жаловался на службу, при этом основная претензия состояла в том, что все сотрудники управления, кроме него, разбирались в компьютерной информации крайне слабо. В результате этот знакомый автора всю работу отдела исполнял сам и в награду выслушивал некомпетентные упреки начальства. Впрочем, начальник, надо отдать ему должное, хотя и не понимал в компьютерах, хотя и поругивал, но не давал в обиду своих подчиненных более высокому начальству, прокуратуре и УСБ. Досидев наконец до пенсии, он ушел. Понятно, что рассчитывать на повышение единственному грамотному специалисту не стоило – не выслужил положенного срока. Прислали нового начальника. Это был старый и опытный кадр. Хорошо зарекомендовавший себя на предшествующей должности – командира конвойного батальона. Учитывая, что до пенсии ему оставалось еще долго, знакомый с сожалением покинул службу, после чего в этом «К» не осталось вообще ни одного сотрудника, знающего, что такое IP-адрес.

Изучение имеющихся трудов в данной области показало, что значимые книги по компьютерной криминалистике издавались только в США (см. список литературы). На русском языке вышло несколько мелких работ [8, 9, 10], при чтении которых автор постоянно испытывал экстремальные эмоции: над юридической их частью плакал, над технической – смеялся. Когда, например, атрибутом файла называют «расширение, то есть примечание, содержащее не более трех символов», это смешно. Но когда средство обхода технических средств защиты авторских прав (ст. 48.1 ЗоАП) объявляют вредоносной программой (ст. 273 УК) – это грустно, и автор сам в период работы над книгой видел на скамье подсудимых не один десяток людей, поплатившихся собственной судьбой за такую вольную трактовку законодательства отечественными «криминалистами».

Вернемся к современному состоянию форензики. Одним из показателей развития является серийный выпуск техники и программного обеспечения, специально предназначенных для сбора доказательств, для обеспечения целостности данных при изъятии и исследовании, для других подобных характерных задач. Номенклатура подобных средств в специализированных магазинах Европы включает около десятка типов, да еще несколько моделей каждого типа. В России такая техника не производится и даже не закупается.

Другим показателем можно считать наличие общественных или межведомственных ассоциаций, обществ, иных профессиональных объединений компьютерных криминалистов или судебных экспертов. Приведем в качестве примера ассоциацию «International Association of Computer Investigative Specialists» (IACIS). Это общественная организация, базирующаяся в США, состоящая из сотрудников правоохранительных органов и занимающаяся преимущественно обучением и просвещением в области форензики. Подобных общественных организаций существует несколько. В нашей стране нет ни одной, нет даже отделения зарубежной. Это говорит о том, что соответствующих специалистов у нас пока мало.

Специальные технические средства

Компьютерный криминалист вполне может обойтись без специальной криминалистической техники вообще. Компьютер сам по себе – достаточно универсальный инструмент. Среди многообразного периферийного оборудования и программного обеспечения найдутся все необходимые для исследования функции. Некоторые программные инструменты можно легко создать или модифицировать своими руками.

Однако специальная техника сильно облегчает работу. Впрочем, карманы она облегчает еще сильнее.

На сегодняшний день на рынке имеются следующие криминалистические инструменты:

- устройства для клонирования жестких дисков и других носителей (в том числе в полевых условиях);
- устройства для подключения исследуемых дисков с аппаратной блокировкой записи на них;
- программные инструменты для криминалистического исследования содержимого дисков и других носителей, а также их образов;
- переносные компьютеры с комплексом программных и аппаратных средств, ориентированных на исследование компьютерной информации в полевых условиях;
- наборы хэшей (hash sets) для фильтрации содержимого изучаемой файловой системы;
- аппаратные и программные средства для исследования мобильных телефонов и SIM-карт [W01, 60, 90];
- программные средства для исследования локальных сетей;
- и некоторые другие.

В целях криминалистического исследования можно эффективно применять не только специально для этого предназначенные средства, но также некоторые средства общего или двойного назначения [W02].

С другой стороны, аппаратные и программные инструменты, которые автор назвал криминалистическими, могут быть использованы не только для правоохранительных целей. У них есть и ряд «гражданских» применений:

- тестирование компьютеров и их сетей, поиск неисправностей и неверных настроек;
- мониторинг с целью обнаружения уязвимостей и инцидентов безопасности;
- восстановление данных, утраченных вследствие неисправностей, ошибок, иных незлоумышленных действий;
- копирование носителей с архивными целями или для быстрой инсталляции/дупликации программного обеспечения;

Серийно выпускаемое криминалистическое компьютерное оборудование

- поиск скрытой или стертой информации для борьбы с утечкой конфиденциальных данных.

Аппаратные средства

Учитывая, что современные компьютеры являются универсальными устройствами, в которых используются в основном открытые стандарты и протоколы, специальных аппаратных средств для исследования самих компьютеров и компьютерных носителей информации не требуется. То есть универсальным инструментом является сам компьютер, а все его функции можно задействовать через соответствующие программные средства.

Немногочисленные аппаратные криминалистические устройства сводятся к дупликаторам дисков и блокираторам записи. Первые позволяют снять полную копию НЖМД* в полевых условиях, но это с тем же успехом можно сделать при помощи универсального компьютера. Вторые позволяют подключить исследуемый диск с аппаратной блокировкой записи на него. Но то же самое позволяет сделать программно любая операционная система (кроме Windows). То есть аппаратные криминалистические устройства для компьютеров и компьютерной периферии служат лишь удобству специалиста или эксперта.

Совсем другое дело – криминалистические устройства для иной техники, отличной от универсальных компьютеров. Мобильные телефоны, цифровые фотоаппараты и видеокамеры, бортовые компьютеры, коммутаторы, маршрутизаторы, аппаратные межсетевые экраны – все эти устройства не являются технологически открытыми и вовсе не стремятся к универсальности. Для полного доступа к компьютерной информации, хранящейся в них, не всегда бывает достаточно компьютера и программных инструментов.

Разнообразие таких устройств соответствует разнообразию выпускаемых электронных устройств, способных нести компьютерную информацию. У каждого производителя – свои проприетарные протоколы, свои интерфейсы. Приобретать такие устройства заранее вряд ли целесообразно. Исключение, пожалуй, составляют ридеры для SIM-карт мобильных телефонов и ридеры для стандартных банковских карт – эти криминалистические устройства всегда полезно иметь в своем арсенале.

Экспертные программы

Такие программы предназначены в основном для исследования содержимого компьютерных носителей информации (прежде всего НЖМД) во время проведения экспертизы.

Они работают не только на уровне файловой системы, но и ниже – на уровне контроллера НЖМД, что позволяет восстанавливать информацию после удаления файлов.

Перечислим несколько популярных экспертных программ:

- Семейство программ ProDiscover (подробнее http://computer-forensics-lab.org/lib/?rid=22)

- SMART (Storage Media Analysis Recovery Toolkit) (http://computer-forensics-lab.org/lib/?cid=18)
- Forensic Toolkit (FTK) фирмы «AccessData» (http://computer-forensics-lab.org/lib/?rid=26)
- Encase – экспертная система
- ILook Investigator (http://www.ilook-forensics.org)
- SATAN (System Administrator Tools for Analyzing Networks) – средство для снятия полной информации с компьютеров для ОС Unix
- DIBS Analyzer 2 (http://www.dibsusa.com/products/dan2.html)
- Helix – экспертный комплект на загрузочном компакт-диске на основе ОС Linux

Наборы хэшей

Так называемые «hash sets» – наборы хэшей – предназначены для облегчения исследования содержимого файловой системы больших носителей, в основном компьютерных жестких дисков.

Предположим, эксперту поступил для исследования изъятый при обыске у подозреваемого НЖМД, на котором установлена операционная система и имеются пользовательские данные. Эти данные могут быть разбросаны по различным директориям, могут содержаться внутри файлов с настройками, даже могут быть скрыты методами стеганографии внутри файлов, содержащих с виду совсем другие данные. Современные ОС включают в свой состав тысячи файлов, популярные приложения – тоже сотни и тысячи. Таким образом, в файловой системе обычного компьютера может находиться, например, 30 000 файлов, из которых только 500 – это файлы, созданные пользователем или измененные им. Чтобы отделить это «меньшинство» пользовательских файлов от заведомо не содержащего ничего интересного «большинства», предназначен набор хэшей.

Хэш, хэш-сумма или однонаправленная хэш-функция* файла представляет собой длинное число, вычисляемое из содержимого файла по особому алгоритму. Хэш-сумма похожа на контрольную сумму, но имеет одно существенное отличие: это однонаправленная функция [18]. То есть по файлу легко вычислить его хэш-функцию, но под заданную хэш-функцию подобрать соответствующий ей файл невозможно.

Хэши известных (то есть входящих в серийное ПО различных производителей) файлов позволяют, не рассматривая подробно содержание этих файлов, отбросить их и быть уверенным, что эти файлы не содержат пользовательской информации. После их исключения эксперту остается исследовать относительно небольшое число файлов. Этот тип наборов именуется «knowngoods».

Существуют и наборы хэшей, выполняющие обратную задачу. Они именуются «knownbads» и соответствуют не заведомо безобидным файлам, а наоборот, заведомо вредоносным, содержащим порнографию, вирусы или иной криминальный контент.

Обычно набор хэшей – это отдельный продукт, приобретаемый у соответствующего производителя (включая подписку на обновления) и подключаемый к экспертному ПО. Он может содержать сотни тысяч и миллионы хэш-функций с соответствующими сведениями о файлах. Все популярные экспертные системы позволяют подключать и использовать «внешние» наборы хэшей.

Архивирование

Копирование и долговременное хранение копий данных сначала применялось лишь с целью восстановления в случае утраты – так называемое «страховочное копирование» или «холодное резервирование».

В последнее время архивирование применяется и с иными целями – для расследования инцидентов безопасности, могущих произойти или обнаружиться в будущем. То есть данные копируются не по принципу «наиболее ценные, наиболее чувствительные данные, утрата которых нанесет ущерб», а по совсем иному принципу: копируются данные и области носителей, где могут оставаться следы злоумышленных действий.

Например, в отношении служебного персонального компьютера для целей восстановления архивируются файлы пользователя и отдельные его настройки. Операционная система и прикладные программы страховочному копированию не подлежат, поскольку легко восстанавливаются из дистрибутива. Все резервное копирование производится на уровне файловой системы. А для целей расследования инцидентов копируется весь жесткий диск (НЖМД) компьютера, причем не на уровне файловой системы, а на уровне контроллера диска, то есть чтобы включалась удаленная и скрытая информация.

Страховочная копия малополезна для расследования инцидентов. Напротив, «инцидентная» копия не подходит для восстановления на случай вирусной атаки или аварии. Это разные копии – и технически, и по назначению. Средства для архивирования на случай расследования инцидентов – это специальные криминалистические средства. Они могут собирать и хранить не только копии НЖМД, но также копии сетевого трафика, копии электронной почты и некоторые другие виды данных.

Значение спецсредств

Следует отметить, что ни одно из криминалистических средств не обеспечивает правильности, корректности, неизменности собранных доказательств, отсутствия их искажений, случайных или намеренных.

Всё упомянутое обеспечивают специалисты или эксперты, применяющие эти средства. Распространенная ошибка при оценке доказательств состоит в том, что придается излишнее значение качествам криминалистической техники (включая ПО), но принижается значение специалистов.

На самом деле ненадлежащие или несовершенные технические устройства вряд ли смогут «испортить» собираемые или интерпретируемые с их помощью цифровые доказательства. В то время как малоквалифицированный специалист – это в любом случае повод усомниться в доказательной силе соответствующих логов, сообщений, иных доказательств в форме компьютерной информации, независимо от того, какими инструментами они были собраны или исследованы.

Бывает, что судья или защитник, желая подвергнуть сомнению доказательства, основанные на компьютерной информации, ставит вопрос о том, какими средствами эти доказательства были собраны, разрешены ли к применению эти средства, сертифицированы ли, не являются ли контрафактными и т.д. Подобная постановка вопроса представляется автору нерациональной. Практика не знает случаев, чтобы судебная ошибка произошла из-за ошибки в криминалистическом программном средстве. Чтобы подвергнуть сомнению цифровые доказательства или результаты компьютерно-технической экспертизы, нужно ставить не вопрос «чем?», а вопрос «кто?». Кто проводил исследование или изъятие компьютерной информации. В практике имеется немало примеров, когда малоквалифицированный специалист, используя «правильные», общепризнанные, должным образом сертифицированные средства, получал «результаты» не просто ошибочные, а не имеющие никакого отношения к исследуемому объекту. Обратных примеров, когда грамотный специалист ошибался из-за использования им «неправильных» криминалистических средств, практика не знает.

Криминалистические информационные системы

Указанные системы не используются напрямую для поиска и изучения доказательств. Они выполняют обеспечивающие функции в работе по раскрытию и расследованию преступлений. Но традиционно относятся к криминалистической технике. Криминалистические информационные системы выполняют ряд близких задач. А именно:

- облегчают и/или ускоряют оформление различных документов для ОРМ, предварительного следствия, судебных целей;
- позволяют работникам правоохранительных органов быстрее найти необходимые нормативные акты, комментарии, прецеденты, получить консультации;

- облегчают и ускоряют доступ сотрудников ко всевозможным базам данных, учетам, справочникам – как публичным, так и закрытым;
- ускоряют и автоматизируют проведение ОРМ, связанных с перехватом сообщений.

Иногда к криминалистической технике причисляют также средства связи и навигации, используемые в работе правоохранительных органов.

Полезно упомянуть следующие информационные системы:

- Глобальная информационно-телекоммуникационная система (ГИТКС) НЦБ Интерпола;
- Единая информационно-телекоммуникационная система органов внутренних дел (ЕИТКС ОВД).

Этапы

Криминалистический процесс, который проводят специалисты и эксперты, принято [11] делить на четыре этапа:

1) сбор;
2) исследование;
3) анализ;
4) представление.

На первом этапе происходит сбор как информации самой по себе, так и носителей компьютерной информации. Сбор должен сопровождаться атрибутированием (пометкой), указанием источников и происхождения данных и объектов. В процессе сбора должны обеспечиваться сохранность и целостность (неизменность) информации, а в некоторых случаях также ее конфиденциальность. При сборе иногда приходится предпринимать специальные меры для фиксации недолговечной (волатильной) информации, например, текущих сетевых соединений или содержимого оперативной памяти компьютера.

На втором этапе производится экспертное исследование собранной информации (объектов-носителей). Оно включает извлечение/считывание информации с носителей, декодирование и вычленение из нее той, которая относится к делу. Некоторые исследования могут быть автоматизированы в той или иной степени. Но работать головой и руками на этом этапе эксперту все равно приходится. При этом также должна обеспечиваться целостность информации с исследуемых носителей.

На третьем этапе избранная информация анализируется для получения ответов на вопросы, поставленные перед экспертом или специалистом. При анализе должны использоваться только научные методы, достоверность которых подтверждена.

Четвертый этап включает оформление результатов исследования и анализа в установленной законом и понятной неспециалистам форме.

Контр-форензика

Противодействие методам поиска, обнаружения и закрепления цифровых доказательств развивается не столь активно, как сама форензика. Дело в том, что спрос на соответствующие контрметоды ограничен. Почему ограничен? Для понимания этого давайте посмотрим, кому и для чего может потребоваться противодействовать обнаружению компьютерной информации.

Во-первых, то, что первым приходит в голову, – киберпреступники. Те, кто имеет основания опасаться закона и прятать следы своей криминальной деятельности. Понятно, что это очень узкий рынок сбыта, работать на нем сложно, крупные высокотехнологичные компании вряд ли станут выпускать оборудование и ПО для этого сегмента, даже если будет спрос.

Во-вторых, контрметоды являются составной частью защиты информации. Везде, где имеется подлежащая защите конфиденциальная информация, должны использоваться методы для предотвращения ее утечки. Часть этих методов по борьбе с утечками ориентированы на исключение или затруднение восстановления информации противником.

В-третьих, право граждан на тайну частной жизни (приватность) может обеспечиваться в числе прочих и компьютерно-техническими мерами, которые фактически являются мерами контркриминалистическими [5, 74]. Правда, применение слишком сложных средств и методов здесь невозможно, поскольку указанная самозащита гражданами своего права на тайну частной жизни ограничена квалификацией среднего пользователя. Соответствующие методы не могут требовать высокой квалификации в области ИТ, соответствующие программы должны быть просты в управлении и работать под ОС «Windows», соответствующее оборудование не может быть дорогим. Поэтому здесь обычно ограничиваются довольно примитивной защитой.

Видно, что значительная часть антикриминалистической техники – непрофессиональная, а то и вовсе кустарная. Видно, что антикриминалистический рынок значительно меньше криминалистического. В случае если антикриминалистическая продукция окажется недоброкачественной, предъявлять претензии к производителю, скорее всего, будет некому. Для преуспевания на этом рынке вовсе не требуется выпускать качественное, сложное оборудование и ПО. Требуется лишь хорошо рекламировать свою продукцию или услуги. Чем производители и занимаются.

К защитным антикриминалистическим средствам можно отнести следующие:

- программы и аппаратно-программные устройства для шифрования хранимой информации;

- программы и аппаратно-программные устройства для шифрования трафика;
- программы для очистки дисков и других носителей;
- устройства для механического уничтожения информации на магнитных носителях;
- программы для сокрытия присутствия информации на диске (манипуляция с атрибутами файлов, запись в нестандартные места, стеганография);
- системы и сервисы для анонимизации сетевой активности;
- программы и аппаратно-программные устройства для затруднения копирования произведений, представленных в цифровой форме, затруднения исследования исполняемого кода и алгоритмов программ.

Многие из названных средств будут описаны ниже.

Противодействие указанным средствам также является задачей форензики.

Заключение

Автор должен признаться, что русский термин «форéнзика» пока нельзя признать устоявшимся. Наряду с ним используются также «компьютерная криминалистика» и «компьютерная форензика». Даже в английском, откуда произошло заимствование, нет полного единообразия: «computer forensics», «digital forensics» и «network forensics».

Тем не менее автор полагает приемлемым использовать слово «форензика» без обязательных оговорок. Новая наука обычно сама для себя выбирает название, то есть название дисциплины (как и вся прочая специфическая терминология) зависит от того, как ее будут называть исследователи-первопроходцы, к числу коих автор и надеется быть причисленным.

1. Компьютерные преступления

Что такое «компьютерное преступление»?

Уголовный кодекс РФ содержит три состава преступлений, называемых преступлениями в сфере компьютерной информации, – ст. 272, 273 и 274 (глава 28). Термин же «компьютерные преступления» несколько шире, чем «преступления в сфере компьютерной информации». Он также охватывает те преступления, где компьютерная техника, программы, компьютерная информация и цифровые каналы связи являются орудиями совершения преступления[1] или объектом посягательства. К таким преступлениям относятся: мошенничество с применением банковских карт (кардинг*), мошенничество с выманиванием персональных данных (фишинг*), незаконное пользование услугами связи и иной обман в области услуг связи (фрод, кража трафика), промышленный и иной шпионаж, когда объектом являются информационные системы, и т.д.

В разных источниках имеется несколько определений «компьютерного преступления» – от самого узкого (только три вышеупомянутых состава) до самого широкого (все дела, касающиеся компьютеров). Для целей форензики четкого определения компьютерного преступления и не требуется. Форензика как бы сама есть определение. Компьютерным можно называть любое преступление, для раскрытия которого используются методы компьютерной криминалистики.

В зарубежной литературе и во многих официальных документах кроме/вместо «computer crime» также часто употребляется термин «cyber crime» – киберпреступность, киберпреступление. Определения этого термина разные, более широкие и более узкие.

Для целей настоящей книги мы будем использовать следующее определение.

Компьютерное преступление (киберпреступление) – уголовное правонарушение, для расследования которого существенным условием является применение специальных знаний в области информационных технологий.

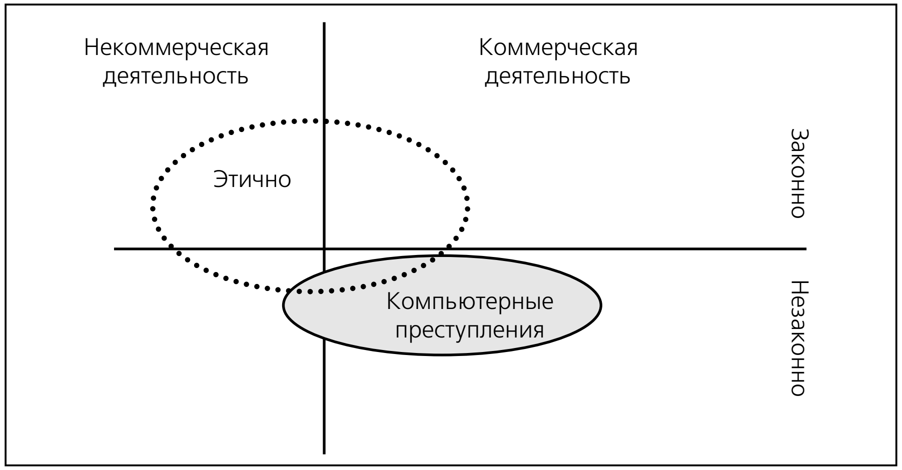
Компьютер и компьютерная информация могут играть три роли в преступлениях, которые автор относит к компьютерным:

- объект посягательства;
- орудие совершения;
- доказательство или источник доказательств.

Во всех трех случаях требуются специальные знания и специальные методы для обнаружения, сбора, фиксации и исследования доказательств.

---

[1] Понятно, что из разряда компьютерных следует исключить такие преступления, где компьютерная техника используется не в качестве таковой, а всего лишь как материальная ценность, тяжелый объект, потребитель электроэнергии и т.п.



«Правовое поле»

Избыточная криминализация

Не всякое общественно опасное деяние объявляется уголовно наказуемым. Некоторые из них государство предпочитает не криминализировать, поскольку тогда не будет возможности соответствующие преступления раскрывать, расследовать и осуществлять правосудие – настолько их будет много. Например, употребление алкоголя – очевидно, что общественно опасно. Многие страны в свое время пробовали вводить сухой закон, но никто в этом не преуспел. То есть бессмысленно бороться уголовно-правовыми методами с массовыми явлениями, для которых никак не хватит производительности у существующих правоохранительных и судебных органов. Однако в отношении некоторых общественно опасных деяний такая логика не принимается во внимание законодателями. В результате в Уголовном кодексе РФ немало составов, расследований по которым не проводится, даже если есть заявление от потерпевшего. Или еще хуже – расследования проводятся лишь по избранным случаям из массы аналогичных. В качестве примера можно привести распространение порнографии (ст. 242 УК) или нарушение тайны связи (ст. 138 УК).

Существуют разные точки зрения на вопрос, следует ли криминализировать общественно опасное деяние, если заранее известно, что не хватит производительности правоохранительных органов на уголовное преследование. С одной стороны, сам факт криминализации и редкие случаи привлечения к ответственности несколько уменьшат количество проявлений. С другой стороны, очевидная для всех необязательность и неисполняемость одного закона будет способствовать неисполняемости других.

К большому сожалению, значительная часть компьютерных преступлений относится именно к таким деяниям – криминализированным, но не обеспеченным ресурсами для раскрытия и расследования. Причем ресурсов не просто не хватает, не просто меньше, чем требуется. Их много меньше, чем нужно для полноценного уголовного преследования соответствующих преступлений. То есть их не хватило бы даже на малую часть, даже при идеально функционирующих правоохранительных органах.

В этой ситуации для работников правоохранительных органов не остается иного выхода, кроме как самостоятельно расставлять приоритеты, сообразуясь со степенью общественной опасности преступления и иными обстоятельствами (см. параграф «Приоритетность расследования").

Криминалистическая характеристика

Для тех, кто, успешно сдав экзамен по криминалистике, уже все забыл, напомним: криминалистическая характеристика – это система типичных признаков преступления того или иного вида.

Сталкиваясь в очередной раз с преступлением, следователь или оперуполномоченный вспоминает похожие дела из своей практики, предполагает, что данное преступление – типичное и пытается применять те же самые подходы, методы, способы поиска доказательств, которые уже приносили успех в аналогичных делах. Чем более типично данное преступление, тем скорее такой подход принесет успех. Если же личный опыт невелик, следует обратиться к коллективному опыту коллег. Именно такой формализованный опыт, система знаний о типичном преступлении определенного класса и называется криминалистической характеристикой.

Она включает следующее:

- способ совершения преступления, предмет посягательства;
- личность вероятного преступника и вероятные его мотивы;
- личность вероятного потерпевшего;
- механизм образования следов;
- обстановка и другие типичные обстоятельства.

В литературе имеется несколько вариантов состава криминалистической характеристики, у разных криминалистов разные представления о необходимой степени ее подробности. Но все варианты более-менее похожи. Автор будет придерживаться вышеуказанного состава.

Большинство исследователей [8, 12, 41] пишет о криминалистической характеристике трех видов преступлений, деля все рассматриваемые преступления по составам трех статей УК – 272, 273 и 274. Вряд ли стоит настолько обобщать. Одной «компьютерной» статьей УК охватывается сразу несколько преступных деяний, сильно отличающихся по личности

преступника, по способу, по оставляемым следам. Например, психически неуравновешенный программист создал и распустил по Сети вирус, чтобы навредить всему миру, который он ненавидит. Другой пример: сотрудник рекламного агентства использует зомби-сеть* (ботнет) для рассылки спама* в соответствии с полученным заказом. Оба они совершают преступление, предусмотренное статьей 273 УК – создание или использование вредоносных программ. Но что может быть общего в характеристиках этих двух преступлений?

Некоторые юристы договариваются даже до того, что рассматривают обобщенную криминалистическую характеристику для всех трех упомянутых составов [40].

В российском УК только три статьи, описывающих преступления в сфере компьютерной информации. В украинском УК – тоже три, в белорусском – семь, в казахском – одна, в киргизском – две, в эстонском – семь. При этом составы, по большому счету, одни и те же. Почему же криминалистических характеристик должно быть непременно три?

Разумеется, при анализе отталкиваться надо не от статей УК, а наоборот – группировать преступления по признаку общности их криминалистической характеристики.

Обсудим отдельные элементы криминалистической характеристики, а затем более подробно – криминалистическую характеристику каждого из видов компьютерных преступлений.

Статистика

Поскольку криминалистическая характеристика выводится из опыта, требуется большое количество совершённых и расследованных преступлений каждого типа. С компьютерными преступлениями дело обстоит не так, как с квартирными кражами или угонами автотранспорта. Их совершается относительно немного, а выявляется и расследуется – и того меньше. Поэтому приведенную в источниках статистическую информацию следует воспринимать не как свыше данную истину, а лишь как первое приближение к будущим характеристикам, которые появятся после накопления значительного опыта.

Кстати, об опыте. Некоторые авторы приводят в криминалистической характеристике статистические данные о личности преступника или обстановке. Например, столько-то процентов преступников моложе 25 лет, столько-то процентов из них мужского пола, такая-то часть работает в отрасли ИТ и связи и т.д. Автор считает подобную статистику несостоятельной. Как полагают все эксперты (и критикуемые источники в том числе), бóльшая часть компьютерных преступлений остается латентной. Раскрывается меньшая часть из них, причем раскрываются лишь простейшие их виды. А криминалистическая характеристика относится ко всем преступлениям – и простым, и сложным. Статистика же подсчитывается только по раскрытым.

Возьмем для примера такой сложный вид преступления, как построение зомби-сетей*. Он должен квалифицироваться по статье 273 УК. Однако раскрытий такого рода преступлений в России вообще не было, а по всему миру было 3 или 4 случая. А теперь подумаем, какое значение для поиска «зомбиводов» будет иметь утверждение, что «40% преступников имели среднее специальное образование»? Учитывая, что статистика эта подсчитана только по раскрытым эпизодам ст. 273 УК, а из них около 3/4 – это навешивание 273-й статьи «в нагрузку» к нарушению авторских прав (строго говоря, неправомерное).

В данной работе автор не только отказался от классификации компьютерных преступлений по статьям УК, но и не использует для криминалистической характеристики судебно-следственную статистику. Автор, сам служивший в органах внутренних дел, слишком хорошо знает, как эта статистика пишется...

Личность вероятного преступника

Оценивая вероятного преступника, важнее всего для нас установить уровень его компетенции в области ИТ. Этот параметр является критическим. В технических методах борьбы, в соревнованиях «спрятать-найти» или «стереть-восстановить» уровень специальных знаний является решающим.

Когда квалификация подозреваемого неизвестна, ее следует предполагать высокой.

С той же целью специалисту или следователю имеет смысл до поры скрывать свой собственный уровень познаний в ИТ перед подозреваемым.

Приведем пример. Изымая компьютер во время обыска (если застали его включенным), специалист должен решить, следует ли применить штатную процедуру выключения или выключить компьютер грубым прерыванием электропитания. С одной стороны, при грубом обесточивании может пропасть некоторое количество данных, как правило, не очень существенных. Но лучше бы их сохранить. С другой стороны, у некоторых хакеров* (в дурном значении этого слова) есть противная привычка оснащать свой компьютер логической бомбой*, срабатывание которой связано с командой выключения компьютера (shutdown). Поэтому при использовании штатного выключения есть риск уничтожить все улики собственными руками. Какой вариант выбрать, зависит от того, как мы оцениваем уровень квалификации владельца компьютера. При невозможности оценить этот уровень компьютер выключается прерыванием электропитания, то есть в расчете на наличие логической бомбы.

Далее приведем описание нескольких типичных образов компьютерных преступников.

«Хакер» (наименование условное). Основной мотивацией этого типа нарушителей являются: исследовательский интерес, любопытство, стремление доказать свои возможности, честолюбие. Средства защиты компьютерной информации, ее недоступность они воспринимают как вызов своим способностям. Некоторые исследователи [12. С. 31-39] полагают необходимой чертой этого типа хорошие знания в области ИТ и программирования. Однако практика опровергла это предположение. Среди обвиняемых по соответствующим составам средний уровень знаний оказался невысок. Другие исследователи [4, 11, 57] наряду с многознающими «хакерами» вводят отдельную категорию «script kiddies*». Это те, кто движим теми же мотивами, но не в состоянии придумать свое и поэтому просто бездумно используют готовые инструменты, сделанные другими. Автор полагает возможным объединить их в единую категорию, поскольку мотивы одинаковы, а знания – вещь наживная.

Первой чертой личностью «хакера» является *эскапизм* – бегство от действительности, стремление уйти от реальности, от общепринятых норм общественной жизни в мир иллюзий, или псевдодеятельность. Компьютерный мир, особенно вместе с Интернетом, является прекрасным альтернативным миром, в котором возможно найти интересное занятие, защиту от нежелательных социальных контактов, реализовать креативный потенциал и даже заработать денег. С другой стороны, человек, который чем-то сильно увлечен в реальном мире, вряд ли сможет найти достаточное количество времени и сил, чтобы стать хорошим специалистом в специфических областях ИТ.

Эскапизм является предрасполагающим фактором для возникновения компьютерной или сетевой зависимости [13]. Такая зависимость (в слабой или сильной форме) является второй чертой личности вероятного преступника. Компьютерная зависимость (аддикция) может начаться с обычного увлечения, которое аддикцией не является. Зависимость в более тяжелой форме ближе к психической девиации, а в тяжелой форме некоторые полагают такую аддикцию болезнью (причем эпидемического характера), которую следует лечить. Исследованию феномена компьютерной/сетевой зависимости посвящены десятки научных работ, как из области медицины, так и социологии [14-17]. Компьютерная, или сетевая аддикция характеризуется неспособностью человека отвлечься от работы в Сети, раздражительностью при вынужденных отвлечениях, готовностью пренебречь ценностями (материальными и социальными) реального мира ради мира виртуального, пренебрежением своим здоровьем. Исследования показывают, что

страдающие сетевой зависимостью люди в то же время отличаются высоким уровнем абстрактного мышления, индивидуализмом, интровертностью, эмоциональной чувствительностью и некоторой степенью нонконформизма.

Эти черты приводят к тому, что «хакер» имеет узкий круг общения и предпочитает всем другим контактам сетевые. Искать его сообщников и источники информации о нем следует прежде всего среди его виртуальных знакомых. Контакты и социальные связи в реальном мире «хакер» субъективно оценивает как менее комфортные и не склонен доверять своим офлайновым* знакомым.

Другое следствие эскапизма – неуделение внимания многому, что существует лишь в реальном мире и никак не отражено в Сети. Например, такой специалист может довольно чисто уничтожить следы, оставляемые на компьютерных носителях (всевозможные компьютерные логи, временные файлы, информацию в свопе и т.д.), но ему даже не придет в голову мысль про логи телефонных соединений, с помощью которых он выходил в Сеть. Один знакомый автору подозреваемый вполне серьезно утверждал, что его преступление «абсолютно недоказуемо», поскольку все мыслимые следы уничтожены. Но преступление оказалось «абсолютно доказуемым», поскольку подозреваемый отчего-то совершенно забыл про существование пяти свидетелей, которым сам же всё подробно описывал и показывал.

Второй чертой личности является некриминальная в общем направленность мыслей «хакера». Исследовательский интерес и честолюбие редко сочетаются с антиобщественными установками, предельной опасливостью, боязнью правоохранительных органов. Это, как правило, выливается в уделение малого внимания заметанию следов, непринятие мер конспирации. Часто у него даже отсутствует само осознание того факта, что совершается уголовное преступление.

Следует упомянуть, что эскапизмом и сниженной социализированностью страдает большинство ИТ-специалистов. Собственно, некоторый отрыв от реальной жизни – это побочный эффект большого опыта в компьютерной сфере. Поэтому поиск по указанным критериям даст не только возможного преступника, но и вполне законопослушных ИТ-специалистов.

«Инсайдер» (наименование условное). Несколько более распространенным типом компьютерного злоумышленника является человек, не слишком хорошо владеющий знаниями в области ИТ, зато владеющий доступом в информационную систему (ИС) в силу служебного положения. Уже стало общим местом утверждение, что бóльшая часть «взломов» компьютерных систем совершается изнутри. Это действительно так. По-

этому при расследовании неправомерного доступа «инсайдер» – первая версия, которую следует рассматривать. Даже если неправомерный доступ был явно снаружи, скорее всего, он стал возможным из-за сговора с местным сотрудником.

Если для «внешнего» хакера обнаружить уязвимость в информационной системе представляет собой задачу, то для сотрудника предприятия почти все уязвимости видны с самого начала. И если информационная система (ИС) имеет отношение к деньгам, ценностям или платным услугам, то сотрудник постоянно пребывает под искушением. Однако руководители и даже сотрудники службы безопасности, чьим попечениям доверена такая ИС, часто страдают странным дефектом зрения: они опасаются и уделяют внимание защите от внешних злоумышленников и в то же время слепо доверяют собственным сотрудникам, забывая, что разница между первыми и вторыми – только в их возможностях. У сотрудников возможностей напакостить несравненно больше.

Итак, типичный «инсайдер» совершает компьютерное преступление (лично или в форме подстрекательства, совместно с «внешним» соучастником) с использованием сведений, полученных в силу служебного положения. Такие сведения – пароли, знания о конфигурации ИС, знания о ее уязвимостях, о принятых процедурах. В ряде случаев этими сведениями он владеет «официально», то есть они ему необходимы для выполнения работы. Но чаще бывает, что реальный доступ сотрудников к конфиденциальной информации значительно шире, чем формальный или чем необходимый. То есть «инсайдер» знает об ИС больше, чем ему положено.

Например, в одной компании-операторе связи имел место инцидент с неправомерным доступом в базу данных. Были изменены данные об объеме оказанных клиенту услуг, от чего компания понесла существенные убытки. Как оказалось, преступником являлся один из сотрудников, вступивший в сговор с клиентом, с которого и «списал» часть задолженности за услуги. Он имел свой собственный логин* в указанную базу данных, но предпочел воспользоваться логином своего начальника. Это не составило особого труда, поскольку тот держал пароль на листочке, приклеенном к монитору. Свалить вину на коллег – характерное поведение для «инсайдера».

Указать иные признаки личности вероятного преступника типа «инсайдер» автор не берется. Некоторые исследователи полагают [39, 40, 48], что «инсайдер» непременно должен считать себя обиженным, обойденным по службе, недостойно вознаграждаемым. Как ни странно, но среди современного «офисного планктона» таковыми считают себя почти все. А среди так называемых «топ-менеджеров» (а равно «стук-менеджеров» и «гарк-менеджеров») – через одного. Если есть искушение украсть, и человек этому искушению поддался, он сам себе осознанно или неосознанно найдет «обиды», вспомнит о «недоплате», о социальной розни и сочинит другие оправдания. Поэтому автор полагает, что такая черта личности вероятного преступника, как наличие обид, в криминалистической характеристике является излишней.

«Белый воротничок» (наименование условное). Этот тип преступника представляет собой давно и хорошо известного казнокрада, но только сменившего инструменты своей деятельности на компьютер. Украсть у государства или у частной компании можно сотней способов. Кроме банального хищения здесь возможны взятки, коммерческий подкуп, незаконное использование информации, составляющей коммерческую тайну, различные виды мошенничества и так далее. В отличие от «инсайдера», этот тип злоумышленника имеет минимальную квалификацию в сфере ИТ и компьютер как орудие совершения преступления не использует. Компьютер здесь выступает только как носитель следов, доказательств совершения преступления.

По своим мотивам «белые воротнички» могут быть разделены на три группы:

1. Злоупотребляющие своим служебным положением из чувства обиды на компанию или начальство. Их следует искать среди долго проработавших сотрудников. Причем для возникновения мотива мести совсем не обязательно наличие действительной обиды со стороны работодателя. В значительной части случаев, как отмечалось выше, обиды эти оказываются вымышленными. Такой обиженный, обойденный и недостойно оплачиваемый злоумышленник чаще всего ворует, чтобы «компенсировать» якобы недополученное от работодателя. Но бывают и бескорыстные мстители, которые не приобретают выгоды от своих незаконных действий либо по этическим соображениям (реже), либо для снижения вероятности раскрытия преступления (чаще).

2. Беспринципные расхитители, не имеющие моральных барьеров и ворующие только потому, что представилась такая возможность. Для подобных «белых воротничков» характерен недолгий срок службы на должности до начала злоупотреблений. Довольно часто за таким имеется криминальное прошлое.

3. Квазивынужденные расхитители, попавшие в тяжелое материальное положение, в материальную или иную зависимость от лица, требующего совершить хищение или мошенничество. Как правило, подобные проблемы трудно скрыть от окружающих – крупный проигрыш, наркомания, семейный кризис, неудачи в бизнесе. Эта группа расхитителей менее осторожна, они не могут долго подготавливать свои преступления, как это делают первые и вторые.

«Е-бизнесмен» (наименование условное). Этот тип вероятного преступника не является квалифицированным ИТ-специалистом и не имеет служебного положения, которым можно злоупотребить. С самого начала он планирует именно криминальное предприятие, отлично осознаёт его противозаконность. Решение совершить правонарушение именно в компьютерной (сетевой) среде, а не в офлайне* он принял не из-за своих особых знаний в этой области и не из-за внутренней тяги к компьютерам, а исключительно на основе рационального анализа. Он посчитал, что так будет выгоднее.

«Выгода» компьютерного преступления обычно связана с его технической или организационной сложностью. На простые уловки попадается мало жертв, от простых средств нападения большинство информационных систем давно защищены. Успешные компьютерные преступления отличаются технической сложностью, участием нескольких сообщников с «разделением труда», многоходовостью. Поэтому чертой личности «е-бизнесмена» является наличие организаторских способностей и предпринимательской инициативы.

Что же касается его незаконопослушности, асоциальности, нонконформизма, то автор полагает эти характеристики не обязательными. На этапе начального накопления капитала, в условиях так называемой «переходной экономики» многие виды бизнеса предусматривают те или иные нарушения законодательства и асоциальную направленность. С этой точки зрения владелец зала игровых автоматов не более асоциален, чем отмывающий деньги через онлайн-казино. А оптимизатор налоговых платежей не менее законопослушен, чем отмыватель электронных кошельков.

Указанному типу преступников отвечает большинство кардеров*, спамеров* и фишеров*.

«Антисоциальный тип» (наименование условное). Также отмечались интернет-мошенники, которые руководствовались не только извлечением прибыли. Более того, их преступный доход часто бывал меньше, чем средняя зарплата специалиста той же квалификации. Мотивом для совершения мошенничества являлась антисоциальная психопатия (социопатия) таких лиц и их патологическая тяга к ведению подобных «игр». Социопатия признана отдельным видом психического расстройства [61, W27] и зарегистрирована под названием «antisocial personality disorder» или «dissocial personality disorder» в классификаторе болезней ВОЗ (ICD, №F60.2). Обычно такие типы действуют импульсивно и не склонны к планированию, особенно долгосрочному.

Подобное расстройство вообще часто приводит к совершению преступления, не только компьютерного, причем мошенничества чаще, чем насилия. Интернет-мошенничество не требует особых технических знаний, вполне достаточно умения пользоваться готовыми программными инструментами.

Оперативность

Некоторые отмечают особое значение оперативности действий при раскрытии и расследовании компьютерных преступлений. Ссылаются на относительно быструю по сравнению с другими видами преступлений утрату доказательств, а также на оперативность связи между сообщниками, которые могут быстро предпринять действия по уничтожению улик и иному воспрепятствованию следственным органам.

Давайте посмотрим, действительно ли это так.

Компьютерная информация бывает короткоживущей. Бывает она и долгоживущей. Даже всерьез говорят [W03] о компьютерной археологии (цифровой археологии), то есть поиске и изучении «древней» компьютерной информации ради получения исторических и обществоведческих сведений. Неоднократно отмечались случаи, когда человек, казалось бы, безвозвратно утративший информацию со своего компьютера, находил ее в Сети и таким образом восстанавливал.

Логи* хранятся не вечно. Но насколько долго? Здравый смысл подсказывает, что хранить их стоит до тех пор, пока они могут пригодиться. В зависимости от содержания логов, этот период полезности соответствует периодичности подсчета статистики, сроку действия клиентского договора, периодичности оплаты услуг, сроку исковой давности. В некоторых случаях длительность хранения логов установлена нормативными актами. Например, постановление Правительства РФ №538 [L01] устанавливает трехлетний срок хранения сведений об абонентах и их «расчетах за оказанные услуги связи, в том числе о соединениях, трафике и платежах». Многие предприятия хранят логи до истечения сроков исковой давности. Некоторые хранят информацию столько времени, на сколько хватает места на диске. В общем, сроки хранения во многих случаях могут быть весьма значительными и даже превышать сроки хранения бумажных документов. В отличие от бумажных, электронные документы обходятся в хранении и обработке несравненно дешевле.

Что касается оперативной связи между сообщниками по компьютерным преступлениям, то все используемые ими способы связи никак не оперативнее обычного телефона, которым пользуются все преступники на протяжении последних десятилетий. Вспомним также об отнюдь не повсеместном доступе к компьютеру и к Сети, об относительно медленной электронной почте, о разнице во времени между сообщниками из разных стран. Заключим в результате, что для среднего «компьютерного» преступника скорость связи с сообщниками вряд ли отличается от скорости связи для среднего мошенника или взяточника.

Возможность быстрого уничтожения цифровых следов и прочих доказательств в ряде случаев, безусловно, присутствует. Стереть один файл можно столь же быстро, как смыть в унитаз один грамм героина. Но вот стирание (а тем более, затирание с гарантией от восстановления) содержимого всего диска занимает десятки минут. В случаях, когда информация находится на удаленных компьютерах, добавляется еще время получения доступа к ним. Уничтожить основные доказательства такого занятия, как фишинг*, займет не один час, если не позаботиться обо всем заранее. Вспомним, что могут успеть за один час преступники, совершившие офлайновые преступления: выбросить в реку пистолет, заменить капот и радиатор после наезда на пешехода, отдать родственнику полученные в виде взятки деньги, выстирать испачканную кровью одежду, сжечь фальшивый паспорт, иногда даже убрать сообщника.

Видно, что оперативность действий по фиксации и изъятию доказательств для расследования компьютерных преступлений столь же важна, как для многих иных преступлений. Поэтому отличительной особенностью компьютерных преступлений не является.

Для иллюстрации темы оперативности вот случай, рассказанный сотрудником управления «К» одного из субъектов Федерации.

Был выявлен и доставлен в управление подозреваемый в совершении неправомерного доступа (ст. 272 УК). После установления места его жительства одного из сотрудников срочно отправили туда для проведения неотложного (ч. 5 ст. 165 УПК) обыска и изъятия компьютера – предполагаемого орудия совершения преступления, на котором надеялись обнаружить основные доказательства. Поскольку для задержания (ст. 91-92 УПК) подозреваемого оснований не нашлось, после допроса он был отпущен домой. На следующее утро оказалось, что в силу некоторых обстоятельств, описывать которые здесь неуместно, упомянутый выше сотрудник так и не произвел обыска в квартире подозреваемого. Разумеется, все подумали, что доказательства с этого компьютера утрачены. Уже без особой спешки, получив судебную санкцию на обыск, отправились к подозреваемому. Была еще слабая надежда, что он по незнанию просто отформатировал свой диск и информацию можно будет восстановить. Каково же было удивление оперативников, когда при обыске они обнаружили не только компьютер подозреваемого с нетронутой информацией, но и еще один компьютер – компьютер сообщника, который подозреваемый принес в свою квартиру, чтобы переписать на него всю ценную информацию со своего. Таким образом, задержка в несколько часов не привела к утрате компьютерной информации, к тому же позволила выявить сообщника.

Конечно, описанный случай не слишком типичный. Но и не единственный в своем роде.

Автор делает следующий вывод. **Необходимость особой быстроты в действиях не является отличительной чертой тактики раскрытия компьютерных преступлений.**

Приоритетность расследования

Ввиду большого количества компьютерных преступлений никто уже всерьез не рассчитывает на возможность расследовать их все. На каких именно фактах стоит сосредоточиться правоохранительным органам и службам безопасности, зависит от следующих факторов:

- Вид и размер ущерба. Очевидно, что более общественно опасными являются те из компьютерных преступлений, которые подразумевают насилие (по сравнению с теми, которые лишь наносят материальный ущерб). Также более приоритетными являются преступления, посягающие на права несовершеннолетних и иных менее защищенных субъектов.
- Распространенность. Как известно, раскрытие преступления и наказание преступника также в некоторой мере воздействуют на потенциальных правонарушителей. Поэтому раскрывать часто встречающиеся типы преступлений при прочих равных важнее, чем редкие типы преступлений.
- Количество и квалификация персонала. В зависимости от того, сколько имеется сотрудников и насколько они квалифицированы, стоит браться за те или иные компьютерные преступления. Слишком сложные начинать расследовать бесполезно.
- Юрисдикция. Предпочтительными являются преступления, не требующие задействовать иностранные правоохранительные органы. Наиболее быстрый результат получается при расследовании преступлений, локализованных в пределах одного города.
- Политика. В зависимости от текущих политических установок, могут быть признаны более приоритетными некоторые виды компьютерных преступлений. Не потому, что они более общественно опасны, но потому, что их раскрытие повлечет больший пиар-эффект или большее одобрение начальства.

Автор вовсе не считает указанную выше приоритезацию целиком правильной, справедливой и подлежащей исполнению. Автор лишь констатирует, как обстоит дело на практике. Потерпевшему, эксперту, специалисту или иному лицу следует учитывать, что правоохранительные органы берутся не за любые компьютерные преступления или проявляют разную степень энтузиазма в зависимости от вышеперечисленных обстоятельств.

Далее рассмотрим самые распространенные виды компьютерных преступлений и дадим их криминалистическую характеристику. Будут описаны лишь те элементы, которые специфичны для рассматриваемого вида компьютерных преступлений.

Как уже указывалось выше, классификация преступлений по статьям УК с научной точки зрения несостоятельна. Одни составы слишком широкие, другие слишком узкие. Например, формулировка статьи 272 охватывает и случай, когда малолетний script kiddie* завладевает копеечным логином* на доступ в Интернет, и случай, когда иностранный шпион получает доступ к компьютеру с государственной тайной. Напротив, статья 187 УК (изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов), казалось бы, специальная статья для кардеров*, охватывает лишь очень незначительную часть кардерской деятельности, в то время как основная деятельность кардеров – это статьи 159 (мошенничество) и 165 (причинение имущественного ущерба путем обмана или злоупотребления доверием).

На основании изложенного автор будет классифицировать компьютерные преступления отнюдь не по статьям УК, а по схожести их криминалистических характеристик.

Онлайн-мошенничество

Способ

Такая форма торговли, как интернет-магазин, нашла широкое применение среди бизнесменов по целому ряду причин. Он, в частности, отличается **низкими затратами** на организацию торговли. Стоимость веб-сайта с соответствующим бэк-офисом* не идет ни в какое сравнение со стоимостью содержания реальной торговой площади. К тому же зависимость текущих затрат интернет-магазина от его оборота если и не очень близка к пропорциональной, то значительно ближе к ней по сравнению с магазином реальным. Это значит, что при отсутствии (нехватке) покупателей убытки будут невелики. Например, цена готового, стабильно работающего интернет-магазина начинается с 15-20 тысяч долларов. По сравнению с реальным (офлайновым*) магазином, тем более в крупном городе, это просто смешные деньги.

Именно эта особенность интернет-торговли привлекла сюда мошенников. Затратив относительно небольшую сумму, злоумышленник может создать видимость нормального торгового предприятия и заняться мошенничеством или обманом потребителей. Десяток-другой жертв вполне окупают сделанные затраты. Для магазина на улице такое было бы немыслимо.

Кроме фиктивных интернет-магазинов мошенники используют и другие предлоги для получения платежей:

- лже-сайты благотворительных организаций, религиозных организаций, политических партий и движений, которые якобы собирают пожертвования;

- спам-рассылки и сайты с просьбой о материальной помощи под трогательную историю о бедной сиротке, жертве войны, заложнике и т.п.;
- сайты фиктивных брачных агентств и отдельные виртуальные невесты;
- мошеннические онлайновые* «банки» и «инвестиционные фонды», обещающие дикие проценты по вкладам;
- рассылки и сайты о якобы обнаруженных уязвимостях и черных ходах в платежных системах, позволяющие умножать свои деньги, например, переслав их на особый счет (в том числе мошенничества II порядка, построенные на том, что жертва думает, будто она обманывает обманщика);
- мошеннические сайты и рассылки, предлагающие удаленную работу (на такую чаще всего клюют сетевые эскаписты) и требующие под этим предлогом какой-либо «вступительный взнос».

Все такие преступления имеют одну и ту же криминалистическую характеристику и сводятся к размещению информации в Сети, анонимному взаимодействию с жертвой и получению от нее денег с последующим исчезновением из Сети.

Одно из мошеннических писем, полученное автором.

```
Message-ID: <005401c60d0a$bd889c4b$ba13f6ba@csuftmeslrimef>
Reply-To: «=?windows-1251?B?zOj14Ojr?=» <ryletsale@37.com>
From: «=?windows-1251?B?zOj14Ojr?=» <ryletsssale@mail.ru>
To: <fnn@optics.npi.msu.su>
Subject: =?windows-1251?B?yuDqIO7h++Pw4PL8IPDz6+Xy6vM=?=
Date: Thu, 29 Dec 2005 21:33:59 +0300
MIME-Version: 1.0
Content-Type: multipart/alternative;
      boundary="----=_NextPart_000_00D6_01C2A75B.03B7B128"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4522.1200
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4522.1200
X-RBL-Warning: mail from 194.67.23.194 refused (RelayWatcher)
X-Lookup-Warning: MAIL lookup on ryletsssale@mail.ru does not match
194.67.23.194
X-MDRcpt-To: fnn@optics.npi.msu.su
X-Rcpt-To: fnn@optics.npi.msu.su
X-MDRemoteIP: 194.67.23.194
X-Return-Path: ryletsssale@mail.ru
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11)
X-Spam-Report:
 * 3.0 MDAEMON_SPAM_BLOCKER MDaemon: message marked by Spam Blocker
 * 0.0 HTML_MESSAGE BODY: HTML included in message
 * 1.2 DATE_IN_PAST_96_XX Date: is 96 hours or more before Received: date
X-Spam-Status: No, hits=4.2 required=5.0 tests=DATE_IN_PAST_96_XX,
 HTML_MESSAGE,MDAEMON_SPAM_BLOCKER autolearn=no version=2.63
X-Spam-Level: ****
```

```
X-Spam-Processed: optics.npi.msu.su, Fri, 29 Dec 2006 21:35:05 +0300
X-MDRedirect: 1
X-MDaemon-Deliver-To: optics@fnn.ru

Я предлагаю вам программу, которая позволит играть в казино и
ВЫИГРЫВАТЬ, абсолютно без риска собственными финансами. Если казино
наживаются на наших страстях, то почему бы и нам не нажиться на их
слабости?! Причем сделать это абсолютно законным способом, без риска
быть уличенным в мошенничестве… Если Вы желаете приобрести программу
для того чтобы использовать ее на практике или просто для всеобщего
развития( программа очень интересная, кроме теории и комбинаций, есть
тренировочная версия игры в рулетку, чтобы вы могли попробовать или
вернее сказать закрепить материал на практике с виртуальными деньгами,
когда вы увидите что система работает, то можете переходить на
настоящую игру. Вышлите 500 рублей с помощью программы яндекс-деньги
на мой счет 4100189014963, затем напишите мне на емайл
ryletsale@37.com
что деньги вы перечислили со своего счета( номер вашего счета и время
перевода) на мой. После этого я в течение 24 часов высылаю вам по
емайл программу. Если Вы боитесь высалать деньги по причине
участившихся обманов, то предлагаю другой вариант Вы пишите на
указанные мною адрес, с возможность ознакомления программой перед
покупкой. Я высылаю ВАМ маленькую часть для ознакомления, если Вас она
заинтересует, то переводите деньги на счет и получаете полностью.
```

Если отвлечься от легенды, то жертвам предлагается перевести 500 рублей при помощи сетевой платежной системы на определенный счет. У мошенника есть минимум сутки на то, чтобы собрать деньги без риска получить обвинение в обмане. Фактически даже больше: при помощи заранее приготовленных правдоподобных оправданий реально растянуть срок до трех суток. Только после этого администрация платежной системы начнет получать первые жалобы на обман.

Предложение разослано при помощи современных спамовых технологий, массово и одномоментно. Из порядка миллиона разосланных копий будут получены от 2 до 4%. Если хотя бы 1% получивших письмо поведутся на обман, мошенник заработает порядка 100 тысяч рублей, что с лихвой покрывает все издержки.

Обстановка

Такие особенности, как **сохранение анонимности** владельца веб-сайта или рассылки и **большой промежуток времени** между приемом заказа и его исполнением, позволяют мошенникам надеяться на успех своего криминального предприятия.

Таким образом, в соответствии с особенностями криминального «бизнес-плана», мы имеем три группы признаков фальшивого интернет-магазина:

- видимая сильная экономия на веб-сайте, рекламе, персонале, услугах связи и другом; мошенник вместо полноценного магазина ограничивается одним лишь «фасадом», дизайн сайта и товарный знак часто заимствованы, заказы обрабатываются явно вручную, не используется банковский счет;
- стремление скрыть личность владельца там, где она должна указываться, – при регистрации доменного имени, приобретении услуг связи, подключении телефонного номера, даче рекламы и т.п.;
- применяются только такие способы оплаты, где возможно скрыть личность получателя платежа, невозможна оплата курьеру при получении;
- период между заказом товара и его доставкой максимально растянут;
- отсутствуют дешевые товары.

Преступник

Вероятны типы преступников: «хакер» и «е-бизнесмен» (см. главу «Личность вероятного преступника»).

Потерпевший

Очевидно, что потерпевший ранее уже пользовался услугами интернет-магазинов, поскольку само использование этого вида торговли для обычного человека непривычно; требуется время, чтобы решиться и привыкнуть покупать товары таким способом.

Столь же очевидно, что потерпевший является пользователем одной из платежных систем, которые использовали мошенники.

Также потерпевшему свойственно до последнего момента надеяться, что его все-таки не обманули или это было сделано неумышленно. Даже через год некоторые из обманутых покупателей все еще могут поверить, что деньги им вернут. Например, уже выявлен и задержан владелец фальшивого онлайн-магазина. Известен один из его клиентов – тот, который и обратился в правоохранительные органы. Чтобы найти остальных потерпевших, имеет смысл возобновить работу веб-сайта, на котором размещался мошеннический магазин и вывесить там объявление с просьбой к жертвам мошенника обратиться к следователю, ведущему дело. Автор уверен, что значительная часть обманутых клиентов все-таки посетит уже давно закрывшийся веб-сайт в надежде, что для них еще не все потеряно.

Следы

Схема всех онлайн-мошенничеств такова:

- размещение (рассылка) информации;
- взаимодействие с жертвой;
- получение денежного перевода.

Все три этапа предусматривают оставление обильных следов технического характера. Хотя мошенники, очевидно, постараются предпринять меры для своей анонимизации. Относительно получения денег мошенников кроме анонимизации спасает быстрота: перевод полученных средств между различными платежными системами осуществляется достаточно быстро, но требует много времени для отслеживания.

При размещении мошенниками подложного интернет-магазина можно рассчитывать на обнаружение следующих видов следов:

- регистрационные данные на доменное имя; логи от взаимодействия с регистратором доменных имен; следы от проведения платежа этому регистратору;
- следы при настройке DNS-сервера, поддерживающего домен мошенников;
- следы от взаимодействия с хостинг-провайдером, у которого размещен веб-сайт: заказ, оплата, настройка, залив контента;
- следы от рекламирования веб-сайта: взаимодействие с рекламными площадками, системами баннерообмена, рассылка спама;
- следы от отслеживания активности пользователей на сайте.

При взаимодействии с жертвами обмана мошенники оставляют такие следы:

- следы при приеме заказов – по электронной почте, по ICQ, через веб-форму;
- следы от переписки с потенциальными жертвами.

При получении денег мошенники оставляют такие следы:

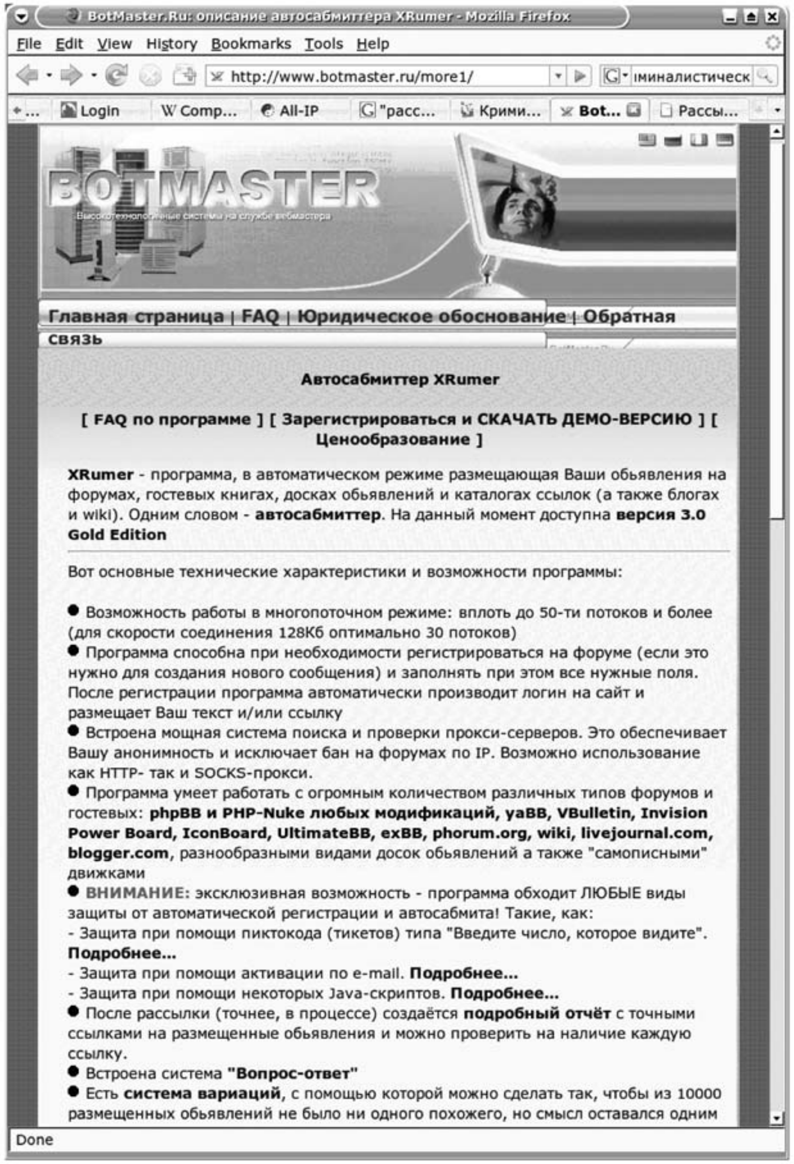
- следы при осуществлении ввода денег в платежную систему (реквизиты, которые указываются жертве);
- следы при переводе денег между счетами, которые контролируются мошенниками;
- следы при выводе денег;
- следы от дистанционного управления мошенниками своими счетами, их открытия и закрытия;
- следы от взаимодействия мошенников с посредниками по отмыванию и обналичиванию денег.

Клевета, оскорбления и экстремистские действия в Сети

Способ

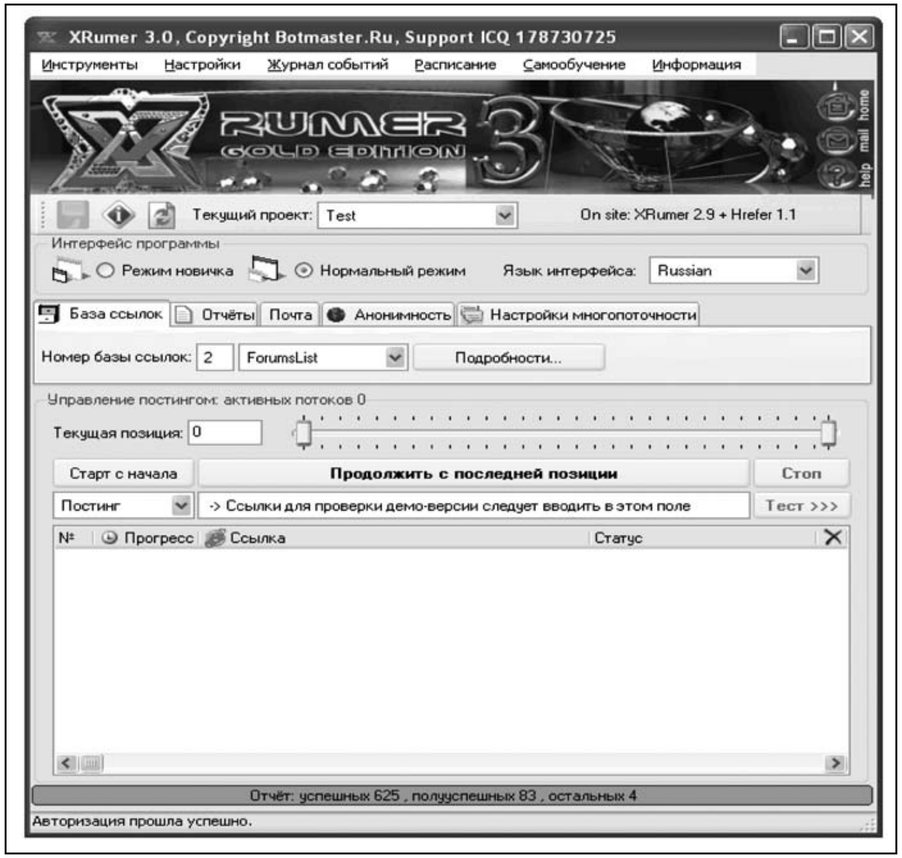
Преступление заключается в размещении на общедоступном, как правило, популярном ресурсе в Интернете оскорбительных, клеветнических или экстремистских материалов.

Ресурсы могут быть следующими: веб-форумы и доски объявлений, веб-страницы*, сообщения в телеконференциях* (newsgroups), массовая



Веб-сайт, предлагающий программу для самостоятельной массовой рассылки (постинга) сообщений по веб-форумам и электронным доскам объявлений

рассылка (спам*) по электронной почте, ICQ, SMS и другим системам обмена сообщениями. Иные средства применяются редко.



Скриншот вышеуказанной программы

В некоторых случаях злоумышленник ограничивается одним-двумя ресурсами. Скорее всего, это непрофессионал, который не может или не хочет оценить охваченную аудиторию. Мало какой ресурс охватывает сразу много пользователей. В других случаях информация размещается на многих ресурсах одновременно, и ее размещение периодически повторяется, как того велит теория рекламы.

Однократное размещение информации злоумышленник может осуществить собственными силами. Для массового размещения ему придется либо привлечь профессионалов-спамеров*, либо найти, подготовить и задействовать соответствующее программное средство для массовой рассылки или спам-постинга.

Предметом посягательства являются честь, достоинство личности, деловая репутация, национальные и религиозные чувства. В некоторых

случаях целью такой кампании может быть провоцирование ложного обвинения другого лица в клевете, оскорблениях, экстремизме; но такое встречается редко.

Преступник

Все эти преступления неспроста объединены в одну главу. У них общий не только способ, но и мотивы. Унижение чести и достоинства физического лица, нанесение ущерба деловой репутации юридического лица, оскорбление национальных и религиозных чувств групп людей – все это, как правило, делается не из корыстных, а из личных побуждений. Дело в том, что сама такая идея – оскорбить, оклеветать, опорочить, поглумиться над национальностью в Сети – может придти в голову лишь сгоряча, человеку, который не привык строить трезвый расчет.

Разумеется, возможны случаи, когда клевета в Интернете – это часть более крупной пиар-кампании, проводимой с определенными корыстными целями. Но такие случаи редки. В России они еще реже.

Когда есть выбор, какую версию предпочесть, «личную», «деловую» или «политическую», лучше начинать с личной. Опыт автора говорит, что большинство правонарушений в Интернете (не только оскорбления, но и DoS-атаки) сейчас диктуются личными мотивами. Корыстные соображения встречаются реже. Деловых людей в Сети пока мало и деловых интересов – тоже. Зато личные обиды и амбиции льются через край.

Понятно из этого, что злоумышленника надо начинать искать среди личных недоброжелателей потерпевшего.

Квалификация типичного преступника для обсуждаемого вида правонарушений находится в четко очерченных рамках.

С одной стороны, он достаточно плотно общается в Интернете, чтобы придавать значение его воздействию на иных людей. Человек, знакомый с глобальной компьютерной сетью лишь поверхностно, вряд ли придаст большое значение тому, что написано на каком-то там веб-сайте. Его круг общения и его референтная группа[1] находятся вне Сети. Его субъективная оценка значимости и достоверности информации из Сети – низкая. К тому же он понимает, что ему будет сложно совершить указанные действия в малознакомой среде.

С другой стороны, уровень знаний о сетевых технологиях такого злоумышленника не может быть высоким, поскольку тогда он осознавал бы, как много следов оставляет каждое действие и сколько есть способов его обнаружить. Новички, попав в Интернет, как правило, опасаются «большого брата» и побаиваются за свою приватность. Пользователь средней

[1] Референтная группа – реальная или условная социальная общность, с которой индивид соотносит себя как с эталоном и на нормы, мнения, ценности и оценки которой он ориентируется в своем поведении и в самооценке.

квалификации уверен, что в Интернете можно легко достичь анонимности, если только принять соответствующие меры. А сетевой профессионал знает, что никакие меры анонимности не обеспечивают.

То есть вероятный преступник довольно много времени проводит в Интернете, но знает о нем не слишком много.

Такое движущее чувство, как обида, обычно развивается постепенно. И если уж подозреваемому пришло в голову разместить клевету или оскорбления именно в Интернете, логично предположить, что там же, в Интернете, его светлое чувство обиды росло и развивалось. Имеет смысл разыскать на веб-сайтах и в переписке предшествующие споры, претензии, негативную информацию, в ответ на которую подозреваемый затеял свою кампанию.

Обстановка

Несколько слов об экстремизме. Признать тот или иной материал экстремистским (равно как возбуждающим межнациональную рознь или, скажем, порнографическим) можно, лишь проведя экспертизу. А до той поры распространение материала защищено правом на свободу слова.

Автору лишь пару раз пришлось видеть в Интернете истинно экстремистский материал, то есть по которому было позже вынесено заключение эксперта. Несравненно чаще приходилось сталкиваться с «экстремизмом» со стороны операторов связи, сотрудники которых отключали клиентов и

Экстремистский веб-сайт, который давно не могут закрыть российские власти.
В настоящее время размещен в Швеции, у провайдера «prq Inet»

закрывали сайты, опираясь исключительно на собственные представления о политике и религии. Подлинная цитата из Правил оказания услуг одного крупного российского хостинг-провайдера: «запрещается размещение информации, пропагандирующей фашизм и коммунизм». Точка.

Был даже случай в практике автора, когда за отключение якобы экстремистского сайта (оценка его содержания произведена исключительно техническими сотрудниками провайдера) было возбуждено уголовное дело против отключившего сайт по статье 144 УК (воспрепятствование законной профессиональной деятельности журналистов), поскольку «экстремистский» веб-сайт был зарегистрирован как СМИ.

Следы

Если размещение информации преступник проводил лично и вручную, следы зависят от способа размещения. Они описаны в разделах 2 и 4.

При размещении информации лично, но с использованием автоматизации будут также следы от поиска, настройки и пробных запусков соответствующей программы. Существуют общедоступные бесплатные и платные программы для рассылки спама по электронной почте, по телеконференциям, для массового постинга в веб-форумы и доски объявлений.

При заказе размещения (рассылки) у специализирующихся на этом профессионалов, то есть спамеров*, искать следы размещения на компьютере подозреваемого бессмысленно. Лучше искать следы его контактов со спамерами: объявления спамеров, переписка с ними, телефонные переговоры, следы подготовки размещаемого текста, перевода денег. Найденные спамеры, если их склонить к сотрудничеству, дадут изобличающие показания, и никаких технических следов размещения информации искать уже не понадобится.

Кроме того, злоумышленник наверняка будет сам просматривать размещенные им тексты как с целью контроля, так и ради отслеживания реакции других. В случае личных некорыстных мотивов он должен испытывать удовлетворение при просмотре своих сообщений. При просмотре образуются соответствующие следы.

DoS-атаки

Способ

DoS-атака* или атака типа «отказ в обслуживании» является одним из видов неправомерного доступа, а именно такого, который приводит к блокированию информации и нарушению работы ЭВМ и их сети. Иные виды неправомерного доступа (копирование информации, уничтожение информации), а также использование вредоносных программ могут быть этапами осуществления DoS-атаки.

Такие атаки принято разделять на два типа [19]: атаки, использующие какие-либо уязвимости в атакуемой системе и атаки, не использующие уязвимостей. Во втором случае своеобразным «поражающим фактором» атаки является перегрузка ресурсов атакуемой системы – процессора, ОЗУ, диска, пропускной способности канала.

Преступник

В настоящее время встречаются DoS-атаки как с личными, так и с корыстными мотивами. Еще 2-3 года назад личные мотивы превалировали [19]. Но сейчас наблюдается четкая тенденция возрастания числа DoS-атак с корыстными мотивами – в целях вымогательства или недобросовестной конкуренции.

Организовать DoS-атаку на типичный веб-сайт не представляет из себя сложной задачи, она под силу ИТ-специалисту средней квалификации, имеющему в своем распоряжении среднее же оборудование и средней ширины канал связи. Соответственно, на черном рынке DoS-атака на обычный веб-сайт стоит десятки долларов за сутки. На более крупный или более защищенный объект – первые сотни долларов за сутки. Возможны оптовые скидки. Заказать атаку может себе позволить даже один обиженный индивидуум. Инструмент для осуществления распределенных DoS-атак – зомби-сети* (ботнеты) – также имеются в продаже на черном рынке по сравнительно низкой цене, порядка десятков долларов за тысячу зомби-хостов. И цена эта в последнее время снижается.

С другой стороны, в Сети появляется все больше и больше чисто информационного бизнеса, благополучие которого целиком и полностью зависит от доступности его сайта или другого сетевого ресурса. Это онлайн-магазины, онлайн-аукционы, онлайн-казино, букмекерские конторы и некоторые другие виды предприятий. Остановка работы веб-сайта в таких условиях означает полную остановку бизнеса. Несколько недель простоя могут полностью разорить предприятие. Естественно, при таких условиях находятся желающие пошантажировать владельца и получить с него выкуп за прекращение DoS-атаки. Несколько лет назад подобных предприятий (е-бизнеса) с существенными доходами еще не было. Соответственно, не было и DoS-вымогательства.

Итак, можно выделить два типа преступлений, связанных с DoS-атаками, – с целью доставить неприятности владельцу или пользователям атакуемого ресурса и с целью получить выкуп.

В первом случае, как и при клевете и оскорблениях, следует искать «обиженного». При этом непосредственным исполнителем может быть как он сам, так и нанятый профессионал.

Во втором случае мы имеем дело с хладнокровным криминальным расчетом, и преступление мало чем отличается от офлайнового вымогательства или недобросовестной конкуренции. Тип возможного преступника «е-бизнесмен» описан выше, в главе «Личность вероятного преступника».

Обстановка

Один тип DoS-атаки основан на использовании уязвимостей в программном обеспечении атакуемого ресурса. Другой тип – так называемый флуд* – не использует никаких уязвимостей и рассчитан на простое исчерпание ресурсов жертвы (полоса канала, оперативная память, быстродействие процессора, место на диске и т.п.). Как легко понять, ко флуду нет неуязвимых, поскольку любые компьютерные ресурсы конечны. Тем не менее разные сайты подвержены флуду в разной степени. Например, CGI-скрипт, работающий на веб-сайте, может быть написан неоптимально и требовать для своей работы слишком много оперативной памяти. Пока такой CGI-скрипт вызывается раз в минуту, эта неоптимальность совершенно незаметна. Но стоит злоумышленнику произвести вызов CGI-скрипта хотя бы сто раз в секунду (никаких особых затрат со стороны злоумышленника для этого не требуется, всего 300 пакетов в секун-

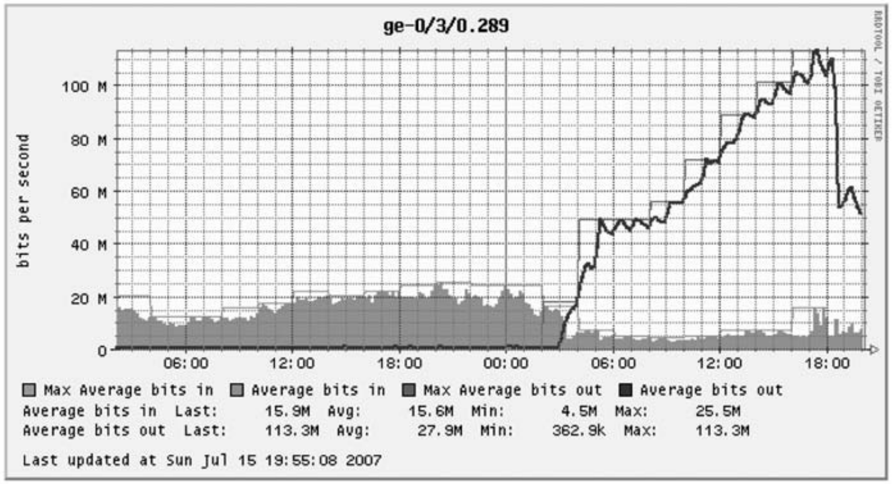


График загрузки канала при DoS-атаке.
Распределенная атака на сайт «Библиотека Мошкова» 15.07.07. Атака представляла собой массу HTTP-запросов, сгенерированных зомби-компьютерами. До 3:00 мы видим характерный веб-трафик: исходящий превышает входящий на порядок. С началом атаки входящий трафик постепенно (не все зомби вводятся в атаку одновременно) возрос с 1 Мбит/с до100 и более. Исходящий же трафик, напротив, упал, поскольку сервер не справляется с нагрузкой. Около 18:00 трафик атаки стал снижаться вследствие предпринятых мер – фильтрации известных адресов зомби-сети

ду, порядка 5 Мбит/с) – и неоптимальность CGI-скрипта приводит к полному параличу веб-сайта.

То есть запас по производительности и есть первичная защита от DoS-атаки.

Обычные хостинг-провайдеры* держат на одном сервере по нескольку десятков клиентских веб-сайтов. По экономическим причинам большого запаса производительности они сделать не могут. Отсюда следует, что типичный веб-сайт, размещенный у хостинг-провайдера, уязвим даже к самому простейшему флуду.

Потерпевший

Потерпевшим в подавляющем большинстве случаев выступает юридическое лицо.

Коммерческие организации редко бывают заинтересованы в официальном расследовании, поскольку для них главное – устранить опасность и минимизировать убытки. В наказании злоумышленника они не видят для себя никакой выгоды. А участие в судебном процессе в роли потерпевшего часто негативно отражается на деловой репутации.

Выступить потерпевшим организация-владелец атакуемого ресурса может в следующих случаях:

- когда есть уверенность, что не наказанный злоумышленник будет повторять атаки;
- когда предприятию надо отчитываться за понесенные убытки или перерывы в оказании услуг перед партнерами, клиентами, акционерами;
- когда руководитель предприятия усматривает в атаке личные мотивы, личную обиду, когда уязвлено его самолюбие.

В прочих случаях не приходится рассчитывать на заинтересованность потерпевшего в раскрытии преступления.

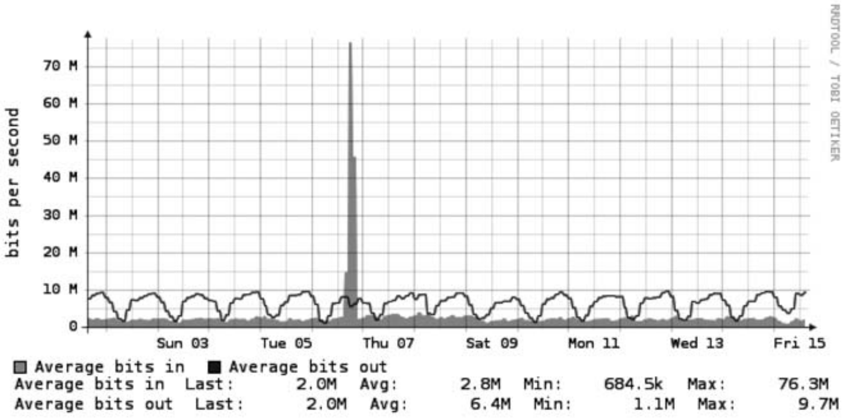
Следует помнить, что многие DoS-атаки воздействуют сразу на целый сегмент Сети, на канал, на маршрутизатор, за которым могут располагаться много потребителей услуг связи, даже если непосредственной целью атаки является лишь один из них. Для целей расследования необходимо установить, на кого именно был направлен умысел преступника. Формальным же потерпевшим может выступить любой из пострадавших от атаки.

Вместо формального потерпевшего мы здесь опишем особенности личности специалиста, который обслуживает атакованную информационную систему и отвечает за ее защиту. Понимание его личности поможет понять причины и механизм совершения преступления.

Типичный профессиональный системный администратор – человек, в реальном мире ничего из себя не представляющий (даже далеко не всегда высокооплачиваемый), но в мире виртуальном – царь и бог. Подобное

двоякое положение сильно способствует развитию комплексов неполноценности и стремлению компенсировать в виртуальности свою ничтожность в реальном мире. Поскольку речь идет о молодом человеке, значительную часть времени вынужденном проводить за компьютером (иначе профессионализм не приобрести), данный комплекс часто усугубляется половой неудовлетворенностью. Теперь представьте, что может натворить такой системный администратор с болезненным желанием продемонстрировать свою власть. При условии, что руководитель компании в технических вопросах вовсе не разбирается или не интересуется ими.

Автор вспоминает случай из своей практики, когда DoS-атака на веб-сайт была заказана одним из посетителей веб-форума на нем. Неосторожное слово, ответная грубость, перепалка – в результате администратор форума закрыл доступ пользователю, которого он считал виновным, и в дальнейшем удалял все его аккаунты. Обиженный решил отомстить. Причем руководствовался, по-видимому, женской логикой, потому что мстить решил не обидевшему его человеку, а веб-сайту. Как выяснилось в ходе расследования, он заказал DoS-атаку на этот сайт. Атака была мощной, а сайт, сервер и сеть в целом не были рассчитаны на большие перегрузки, работали вблизи предела своей производительности. В результате атаки «упал» не только целевой веб-сайт, но и несколько десятков веб-сайтов, живших на том же сервере. А также потеряли работоспособность соседние сервера, использовавшие тот же канал связи. Пострадавшими были: магистральный



Пример исходящей DoS-атаки типа флуд на фоне типичного веб-трафика с дневной периодичностью. В период атаки (серый пик 6 числа) виден провал в профиле входящего трафика (черная линия) – он образуется за счет перегруженности канала

провайдер, у которого оказался целиком забит флудом* канал связи, оператор дата-центра, несколько хостинг-провайдеров, чьи сервера соседствовали с целевым, а также все их клиенты – всего более сотни лиц.

Описанную DoS-атаку было бы значительно легче предотвратить, чем отразить или преодолеть ее вредные последствия. Стоило администратору веб-форума быть немного сдержаннее или хотя бы задуматься о последствиях, и атаки удалось бы избежать.

Можно сказать, что для потерпевшего от DoS-атаки (точнее, сотрудников юрлица-потерпевшего) характерно провоцирующее поведение в онлайновых* взаимоотношениях.

Следы

При подготовке и проведении DoS-атаки образуются следующие следы технического характера:

- наличие инструментария атаки – программных средств (агентов), установленных на компьютере злоумышленника или, чаще, на чужих используемых для этой цели компьютерах, а также средств для управления агентами;
- следы поиска, тестирования, приобретения инструментария;
- логи (преимущественно статистика трафика) операторов связи, через сети которых проходила атака;
- логи технических средств защиты – детекторов атак и аномалий трафика, систем обнаружения вторжений, межсетевых экранов, специализированных антифлудовых фильтров;
- логи, образцы трафика и другие данные, специально полученные техническими специалистами операторов связи в ходе расследования инцидента, выработки контрмер, отражения атаки. (Следует знать, что DoS-атака требует немедленной реакции, если владелец желает спасти свой ресурс или хотя бы соседние ресурсы от атаки. В ходе такой борьбы обе стороны могут применять различные маневры и контрманевры, из-за чего картина атаки усложняется.);
- следы от изучения подозреваемым (он же заказчик атаки) рекламы исполнителей DoS-атак, его переписки, переговоров и денежных расчетов с исполнителями;
- следы от контрольных обращений подозреваемого к атакуемому ресурсу в период атаки, чтобы убедиться в ее действенности.

При профессиональном осуществлении атаки используются зомби-сети* или иной специализированный инструментарий. Естественно, он не одноразовый. Исполнители не заинтересованы в простаивании своих мощностей и могут осуществлять несколько атак одновременно, либо осуществлять теми же программными агентами параллельно с атакой другие функции, например, рассылку спама*.

Дефейс

Способ

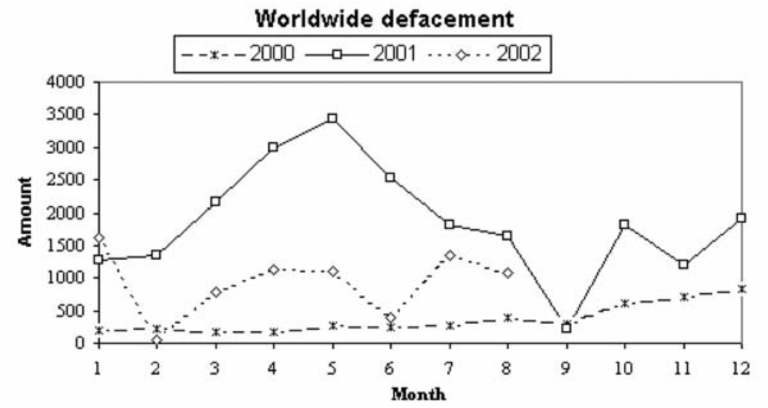
Данное правонарушение состоит в том, что злоумышленник тем или иным способом изменяет внешний вид публичного веб-сайта потерпевшего, чаще всего его титульную страницу. Технически это можно осуществить, получив доступ на запись к директории, где хранятся данные веб-сервера. Также часто дефейс производят, воспользовавшись уязвимостью в самóм веб-сервере или одном из его CGI-скриптов. Бывает, что злоумышленник изменяет веб-страницу, воспользовавшись штатной функцией, под аккаунтом одного из законных пользователей.

Следует отличать дефейс от подмены веб-сайта при помощи атаки на DNS или изменения DNS-записи для сайта жертвы. Это иной способ, хотя цель атаки может быть такой же, как при дефейсе.

Явление это достаточно распространенное. Фиксируются тысячи подобных инцидентов ежемесячно. Можно предположить, что не все дефейсы попадают в статистику, поскольку для владельца взломанного веб-сайта выгодно скрыть такой инцидент.

Дефейс веб-сайта «SCO» 29.11.2004. Сделан, скорее всего, по идеологическим мотивам. Измененная титульная страница прожила около трех часов. О новости сообщили все СМИ, интересующиеся компьютерно-сетевой тематикой

Для сравнения – обычный вид веб-сайта «SCO». Как видно, в данном случае злоумышленник лишь частично изменил внешний вид титульной страницы сайта. В большинстве случаев при дефейсе внешний вид страницы изменяется кардинально



Количество зафиксированных дефейсов в 2000-2002 годах по месяцам. Источник – [65] со ссылкой на www.zone-h.org

Преступник

Мотивы для дефейса бывают следующие (перечислены в порядке убывания частоты):

- стремление продемонстрировать публично свою квалификацию;
- политические, религиозные, иные идеологические мотивы;
- личная неприязнь, личный конфликт с потерпевшим или кем-либо из его работников;
- стремление дискредитировать владельца веб-сайта, испортить ему деловую репутацию в целях конкурентной борьбы, повлиять на его капитализацию в целях биржевой спекуляции;
- стремление продемонстрировать наличие уязвимости в ПО, привлечь к ней внимание.

Вероятный преступник соответствует модели «хакер» или реже – «инсайдер».

Следы

На взломанном компьютере следов остается не много, злоумышленник старается по возможности уничтожить их. Не следует удивляться, если следов там вообще найти не удастся. Больше следов можно найти на компьютерах, которые хакер использует в качестве промежуточных узлов для исследования атакуемого веб-сайта и доступа к нему. Также пригодятся статистические данные транзитных провайдеров (см. главу «Статистика трафика» в разделе 2). А на собственном компьютере злоумышленника следов должно быть еще больше – там должны найтись переработанная или заново изготовленная веб-страница, а также ее промежуточные варианты, средства для осуществления несанкционированного доступа, средства для поиска и эксплуатации уязвимостей на целевом веб-сайте и промежуточных узлах.

Помимо этого, злоумышленнику еще необходимо привлечь общественное внимание к дефейсу. В противном случае акция может остаться незамеченной – измененные сайты недолго остаются в таком состоянии, владелец обычно быстро восстанавливает первоначальный вид.

Следовательно, злоумышленник сразу после «взлома» или незадолго до него каким-либо способом оповестит мир о своем преступлении. Это могут быть сообщения по электронной почте, статья в телеконференции или на веб-форуме. Все эти действия оставят дополнительные следы.

Злоумышленник также будет периодически проверять результат дефейса и отслеживать реакцию общественности на него. Эти действия он может совершать со своего компьютера, без особых мер для анонимизации.

Потерпевший

Чаще потерпевшим является юридическое лицо. Обычно предприятие-потерпевший не заинтересовано в разглашении информации об инциденте. Но если широкая огласка уже произошла, позиция потерпевшего может измениться, поскольку необходимо чем-то компенсировать ущерб деловой репутации и как-то оправдаться перед акционерами и клиентами. Быстро найти и привлечь к ответственности злоумышленника – это все-таки некоторая компенсация в плане репутации и общественных связей.

К данному преступлению относится все, сказанное о потерпевших в предыдущей главе ("DoS-атаки").

Вредоносные программы

Способ

Антивирусные аналитики отмечают явную тенденцию к коммерциализации вредоносного ПО. Еще 5-7 лет назад почти все вирусы и черви создавались без явной корыстной цели, как полагают, из хулиганских побуждений или из честолюбия.

А среди современных вредоносных программ большинство составляют программы, заточенные под извлечение выгоды. Основные их разновидности (с точки зрения предназначения) суть следующие:

- троянские программы для создания зомби-сетей*, которые затем используются для рассылки спама, DoS-атак, организации фишерских сайтов и т.п.; нередко они снабжены механизмом самораспространения;
- так называемое spyware*, то есть черви и троянцы для похищения персональных данных – паролей и ключей к платежным системам, реквизитов банковских карточек и других данных, которые можно использовать для мошенничества или хищения;
- так называемое adware*, то есть вредоносные программы, скрытно внедряющиеся на персональный компьютер и показывающие пользователю несанкционированную рекламу (иногда к классу adware причисляют не только вредоносные, но и «законопослушные» программы, которые показывают рекламу с ведома пользователя);
- руткиты*, служащие для повышения привилегий пользователя и сокрытия его действий на «взломанном» компьютере;
- логические бомбы*, которые предназначены для автоматического уничтожения всей чувствительной информации на компьютере в заданное время или при выполнении (при невыполнении) определенных условий;
- так называемое «ransomware» – подвид троянских программ, которые после скрытного внедрения на компьютер жертвы шифруют файлы, содержащие пользовательскую информацию, после чего предъявляют требование об уплате выкупа за возможность восстановления файлов пользователя.

Следует отметить, что так называемые кряки* – программы, предназначенные для обхода технических средств защиты авторского права, – не относятся ко вредоносным. Как по букве закона, так и по техническим особенностям создания и применения, они стоят особняком. Создание кряков имеет смысл рассматривать отдельно (см. главу «Нарушение авторских прав в офлайне»).

Преступник

Как современная вредоносная программа является лишь средством, технологическим элементом для криминального бизнеса, так и современный вирусописатель работает не сам по себе, а исполняет заказы других. Это может быть прямой заказ, когда программист-вирмейкер* получает техническое задание, исполняет его и отдает готовый продукт заказчику. Это может быть непрямой заказ, когда вирмейкер*, зная потребности черного рынка, старается их удовлетворить своим продуктом, который затем и реализует (лицензирует пользователям) самостоятельно.

Давно не отмечалось случаев, когда один человек исполнял весь преступный замысел целиком – писал вредоносную программу, применял ее, использовал результат применения для извлечения дохода.

Таким образом, создатель вредоносной программы – это почти всегда член преступной группы. Его деятельность не имеет смысла в отрыве от заказчиков и пользователей вредоносной программы.

Кроме создания вредоносных программ уголовно наказуемо и их применение. Лицо, использующее такую программу, тоже в большинстве случаев не реализует результаты своего труда непосредственно, а продает или передает их дальше, другим членам преступной группы.

Наконец, третий тип – это реализаторы результатов применения вредоносных программ, то есть спамеры*, вымогатели, кардеры*, мошенники.

Приведем примеры типичных криминальных «коллективов».

Спамеры. Первый сообщник создает и совершенствует программное обеспечение для скрытного внедрения на компьютеры пользователей (троянцы*). Второй, купив у первого право на использование указанной программы, рассылает ее в массовом порядке, принимает сигналы и учитывает успешно внедрившиеся экземпляры троянцев, объединяет их в структурированную зомби-сеть*. Готовую сеть (целиком или частично, насовсем или на время) он продает третьему сообщнику, который с ее помощью осуществляет рассылку спама. Заказы на рассылки принимает четвертый сообщник, который ищет заказчиков при помощи того же спама, часть полученных от заказчиков денег перечисляет третьему в оплату

его услуг. Пятый занимается сбором и верификацией адресов электронной почты для рассылок. Собранные базы адресов (или подписку на такие базы) он продает либо четвертому, либо третьему сообщнику.

Кардеры. Первый из сообщников (точнее, первая группа, одного человека тут не хватит) занимается сбором атрибутов банковских карт*. Он может служить продавцом или официантом и незаметно снимать данные с карточек клиентов. Он может быть менеджером в фирме или банке и получать доступ к базе данных карточек в силу служебного положения. Он может получать номера карточек, внедряя вредоносные программы-шпионы (spyware) или через фишинг*. Добыв некоторое количество номеров (или даже дампов*) банковских карт, первый сообщник сбывает их второму. Второй исполняет роль организатора криминального бизнеса. Он аккумулирует у себя данные и распределяет их исполнителям. Третий сообщник исполняет по заказам второго верификацию реквизитов карт, то есть проверяет их действительность и пригодность для платежей. Четвертый сообщник создает и поддерживает платный веб-сайт или лжемагазин или интернет-казино* с возможностью оплаты услуг карточками. Он имеет несколько договоров с биллинговыми компаниями, время от времени меняет их, а также свою вывеску. Это механизм для отмывания денег. Пятая группа сообщников – так называемые набивщики. Они получают от второго партии номеров банковских карт по нескольку десятков и вводят их через отмывочное предприятие четвертого сообщника под видом разных клиентов. При этом они должны при помощи технических средств эмулировать доступ из разных стран и с разных компьютеров. За свою работу они получают сдельную оплату, реже – процент с доходов. Шестой сообщник представляет собой иной канал реализации, он занимается так называемым вещевым кардингом. Получая от второго «отборные», наиболее перспективные номера кредиток, он использует их для покупок в настоящих интернет-магазинах. Покупается в основном дорогая, нетяжелая и ликвидная техника – мобильные телефоны, видеокамеры, компьютерные комплектующие, некоторые автозапчасти и т.п. Естественно, заказываются они вовсе не на его адрес. Для получения заказов существует седьмая группа сообщников – дропы. Это граждане из благополучных стран, поскольку большинство интернет-магазинов не доставляют заказы вне США, Канады и ЕС, а если и доставляют, то проверяют таких покупателей очень тщательно. Работа дропов состоит в том, чтобы подтвердить по телефону сотруднику магазина, что заказ сделал он, получить посылку и тут же переслать ее шестому сообщнику (иногда – другому дропу, для пущего запутывания следов). Дропы вербуются десятками из малообеспеченных слоев общества типа студентов или негров. Обычно дроп выполняет всего десяток-другой операций с интервалом в несколько недель. Он получает оплату сдельно или в виде процента от

стоимости товара. Наконец, восьмой сообщник занимается получением и реализацией посылок от дропов.

Фишеры. Первый сообщник занимается размещением подложных веб-сайтов банков и иных учреждений. В состав программ такого сайта входит система для моментальной отсылки введенных клиентом конфиденциальных данных злоумышленнику, естественно, не напрямую, чтобы трудно было его вычислить. Второй изготавливает эти сайты, составляет подложные письма и рассылает их, но не самостоятельно, а пользуясь для этого услугами спамеров*. Третий сообщник занимается реализацией полученных данных (номера карт с пин-кодами или пароли к платежным системам) кардерам или иным криминальным структурам. Бывает, что реализацией пин-кодов преступная группа занимается самостоятельно. Тогда предусмотрен четвертый сообщник, который изготавливает «пластик», то есть копии банковских карт для офлайновых магазинов и банкоматов, а также пятая группа, которая собственно снимает из банкоматов деньги, получая для этого карты и пин-коды у четвертого.

Видно, что вредоносное ПО во всех случаях играет роль инструмента для одного из этапов большого преступного замысла. И создатель, и применитель вредоносных программ также исполняют общий замысел.

Отмечались и иные способы использования добытых при помощи вредоносных программ конфиденциальных данных. Например, в конце 2006 года был зарегистрирован случай массовой кражи атрибутов доступа программы ICQ, которая осуществлена при помощи вредоносной программы, массово разосланной пользователям. «Красивые» номера ICQ через посредников поступили в продажу. А из остальных злоумышленники попытались выжать деньги оригинальным способом. Они под видом прежних владельцев ICQ-аккаунтов обращались к их знакомым (используя контакт-лист, украденный вместе с паролем или скачанный с сайта) и просили денег «взаймы». Есть сведения, что некоторый процент пользователей ICQ откликнулся на такую просьбу.

Итак, вероятный преступник по делам о создании и использовании вредоносных программ – это член преступной группы, работающий в этой группе на основе найма или за процент от дохода или как самостоятельный создатель орудий преступления. То есть с точки зрения экономики вирусописатель продает в одних случаях свою рабочую силу, в других – свой труд, а в третьих – результат своего индивидуального труда.

Как правило, это профессиональный программист, вставший на преступный путь уже после выбора профессии. Его движущим мотивом являются деньги. Мотивы, характерные для типа «хакер», то есть самоутверждение и исследовательский интерес, могут иметь значение лишь на первом этапе, при вовлечении его в преступную деятельность. Корыстный же мотив – всегда основной.

Звонилки (dialers)

Одним из видов мошенничества является недобросовестное использование платных телефонных линий. Абонировав соответствующий номер с высокой оплатой за «разговор» со стороны вызывающего абонента, мошенники всяческими способами пытаются спровоцировать вызовы на него со стороны абонентов. Помещают этот номер в заведомо ложной рекламе, отправляют SMS и совершают исходящие вызовы с этого номера, чтобы абонент перезвонил, сами совершают звонки на свой номер, пользуясь несовершенством биллинга оператора, навязывают ложную информацию о вызовах телефонной сети, а также вставляют (загружают) этот номер во вредоносные программы-звонилки (dialer), которые заставляют модем пользователя совершать вызов.

По условиям договора оператор вызывающего абонента платит за такой звонок оператору вызываемого абонента, а потом пытается получить деньги со своего абонента.

Опишем более подробно один из самых распространенных типов такого мошенничества – с использованием вредоносной программы-звонилки (dialer, диалер, программа дозвона).

Большинство звонилок относятся к классу троянских программ. Одни из них имеют обычный для троянцев механизм скрытного внедрения на компьютер или маскируются под полезные программы. Другие таких механизмов не имеют и рассчитаны на однократный запуск самим пользователем, который введен в заблуждение методами социальной инженерии. Например, на веб-сайте, содержащем многочисленные ссылки на порнографию, некоторые ссылки ведут на такую программу с пояснением «запустите для просмотра видео». Обманутый пользователь кликает на гиперссылку, тем самым скачивая программу-звонилку, и запускает ее. Будучи запущенной, она скрытно внедряется на компьютер пользователя (возможно, при этом даже показывает ему видео) и впоследствии активизируется, набирая при помощи модема платный номер[1]. Злоумышленники получают через оператора деньги за совершенный звонок, а потерпевшему потом предоставляется разбираться со своим оператором связи, доказывая, что он не звонил в Лихтенштейн и не получал услугу «для взрослых».

Следует заметить, что среди подобных программ-диалеров есть и невредоносные, которые не скрывают своего присутствия и своего предназначения и показывают пользователю, какой звонок и по какому тарифу будет произведен. Они также иногда используются для обмана потребителей, но не вызывают столько проблем у абонентов и не влекут обвинения в мошенничестве и в использовании вредоносных программ.

[1] При соединении с таким номером пользователь часто даже получает интернет-соединение и, думая, что соединился со своим провайдером, не замечает подмены и остается на связи долгое время.

Итак, большинство программ-звонилок являются вредоносными, поскольку внедряются на компьютер и производят свои действия без уведомления пользователя и разрешения от него. Многие потерпевшие настаивают на возбуждении уголовного дела по факту заражения такой программой, поскольку считают, что это позволит им не оплачивать стоимость звонка оператору связи.

Но на сегодняшний день суды не признают вредоносные программы стихийной силой, а их действия – форс-мажорными обстоятельствами. Поэтому заразившимся такими программами пользователям все же приходится оплачивать звонки. Впрочем, иногда оператор связи склонен «прощать» такую задолженность абонента – не по закону, а по справедливости.

Одни из программ-звонилок имеют собственный механизм распространения, чаще всего рассылают себя по электронной почте по списку адресов, найденных на зараженном компьютере. Другие самостоятельно распространяться не умеют, и злоумышленник вынужден размещать их на веб-сайтах, маскировать под что-то безобидное и рекламировать свой сайт.

Количество заражений подобными программами медленно снижается, поскольку все меньше компьютеров используют модем, все больше – выделенные линии связи.

Следы

При изготовлении вредоносных программ можно обнаружить следующие цифровые следы:

- исходный текст вредоносной программы, его промежуточные варианты, исходные тексты других вредоносных или двойного назначения программ, из которых вирмейкер заимствовал фрагменты кода;
- антивирусное ПО различных производителей, на котором создатель вредоносной программы обязательно тестирует свою, а также средства для дизассемблирования и отладки;
- программные средства для управления вредоносными программами (многие из них работают по схеме «клиент-сервер», одна из частей внедряется на компьютер жертвы, а другая часть работает под непосредственным управлением злоумышленника);
- средства и следы тестирования работы вредоносных программ под различными вариантами ОС;
- следы контактирования с заказчиками или пользователями вредоносной программы, передачи им экземпляров и документации, оплаты.

При распространении и применении вредоносных программ можно обнаружить следующие цифровые следы:

- средства и следы тестирования работы вредоносной программы под различными вариантами ОС;

- контакты с создателем или распространителем-посредником вредоносной программы;
- программные средства для управления вредоносной программой, данные о внедрениях этой программы к жертвам, результаты деятельности (пароли, отчеты о готовности, похищенные персональные данные);
- средства распространения вредоносной программы или контакты с теми, кто подрядился ее распространять.

Кроме того, на компьютере жертвы должна найтись сама вредоносная программа (ее серверная или клиентская часть). Очень часто обнаруживает ее сам потерпевший при помощи антивирусного ПО. При этом вредоносная программа может быть уничтожена по команде пользователя или автоматически, в соответствии с настройками антивируса. Хотя исполняемый код вредоносной программы, обнаруженный в ходе экспертизы, является доказательством по делу, в случае его уничтожения потерпевшим без этого доказательства можно обойтись. Лог антивируса, а также следы деятельности вредоносной программы, будучи исследованы в ходе экспертизы, позволят эксперту категорично утверждать, что на исследуемом компьютере была установлена определенная вредоносная программа, хотя исполняемого кода этой программы и не обнаружено. Лучше поручить такую экспертизу предприятию, которое производит или обслуживает соответствующее антивирусное ПО.

Кардерство

Способы

Объем мошеннического рынка в области банковских карт* очень велик. Его можно оценить так. В каждом банке установлен лимит приемлемых потерь при карточных операциях. Он колеблется в пределах 0,1-0,5%. Это значит, что не менее 0,1% всего мирового оборота по карточным операциям достается кардерам*.

С банковскими (платежными) картами возможно несколько видов мошенничества. Их всех можно уложить в единую схему:

получение – распределение – реализация

На первом этапе данные о банковских картах получаются разнообразными способами. На втором этапе они сортируются, проверяются, классифицируются, возможно, проходят через оптовых посредников (скупка в розницу, продажа оптом, продажа в розницу). На третьем этапе данные банковских карт реализуются, то есть конвертируются в деньги.

Указанная цепочка никогда не исполняется одним человеком. Каждый из этапов связан со своими особенными навыками, опытом в соответствующей области, служебным положением, доступом к технике. Поэтому криминальная цепочка всегда включает не менее трех сообщников.

Получение

Наборы данных банковских карт, которые представляют ценность:

(1) номер, срок действия, имя владельца, код[1] cvv или cvv2

(2) дамп* карты

(3) дамп + пин-код

Третий вариант – самый привлекательный для кардеров. Этот набор данных можно конвертировать в наличные самым быстрым способом и получить при этом максимальную сумму.

Портативные считыватели, используемые мошенниками для скрытного снятия дампа карты в местах оплаты

Способы получения данных банковских карт:
- дистанционный неправомерный доступ к серверу, на котором такие данные хранятся или обрабатываются, например, к серверу магазина или банка – способ, наиболее часто предполагаемый несведущими людьми, но очень редко встречающийся на практике;
- доступ к таким данным с использованием своего служебного положения и недостатков в системе защиты информации предприятия – очень часто владельцы конфиденциальной информации предпринимают излишние меры защиты от внешних угроз, но пренебрегают защитой от угроз внутренних;
- (редко) перехват интернет-трафика, когда данные карты передаются в открытом виде (по протоколу HTTP или по электронной почте);
- получение данных банковских карт, или снятие дампа* при обслуживании клиентов в предприятиях торговли и питания – похож на пре-

[1] Card Verification Value

дыдущий способ, но особенность в том, что информация копируется непосредственно с карты при физическом контакте с ней;
- выманивание данных карт и иногда пин-кодов у владельцев методами фишинга*;
- получение дампов и пин-кодов при помощи фальшивых банкоматов или приставок к банкоматам (скиминг*);
- получение самой карточки мошенническим способом («ливанская петля» и др.);
- обычная кража карты у ее держателя (бывает, что пин-код записан на ней или на листке, лежащем в том же бумажнике).

Реализация

Реализация данных с банковских карт, то есть обращение их в деньги, может производиться следующими способами:
- вещевой кардинг – приобретение в интернет-магазинах или в реальных магазинах (при наличии дампа карты) ликвидных товаров, чаще на продажу, реже на заказ, последующая их реализация;
- совершение фиктивных покупок в интернет-магазинах или приобретение услуг платных сайтов по сговору с их владельцами; при помощи данных чужой карты производится оплата, биллинговое предприятие* (оно не участвует в сговоре) учитывает платеж и переводит магазину за вычетом своей комиссии, магазин переводит обусловленную долю кардеру;
- игра в интернет-казино*; нанятые кардером игроки регистрируют в интернет-казино много аккаунтов* на имя владельцев карт, вносят с карт депозит, играют, а затем для тех аккаунтов, где образовался выигрыш, проводят процедуру вывода средств;
- использование иных интернет-сервисов, где возможно получение денег, например, организующих показ любительского видео;
- (редко) вымогательство у магазина, банка, иного предприятия, несущего ответственность за сохранность данных; за утрату и разглашение данных о картах клиентов предприятие может подвергнуться санкциям со стороны платежной системы, получить большой ущерб деловой репутации, может стать ответчиком по искам клиентов – за избавление от этих неприятностей многие готовы заплатить кардерам-вымогателям;
- обналичивание в банкоматах; когда есть дамп карты и пин-код, то изготавливается твердая копия карты (так называемый «белый пластик», потому что внешнее оформление для банкомата не требуется), с которой в банкоматах снимается максимально возможная сумма за минимально возможное время.

Ниже приводятся немного более подробные пояснения к перечисленным способам приобретения и реализации данных банковских карт.

Скиминг

Наиболее лакомый кусок для кардеров – это полная копия (дамп) магнитной полосы карты вместе с ее пин-кодом. Такие данные позволяют

Приставка к банкомату, замаскированная под конструктивную часть и осуществляющая скрытное копирование магнитной полосы карты

снять со счета весь остаток средств плюс весь кредитный лимит. Обычно это десятки тысяч долларов. Ради подобного куша кардеры готовы на многое. Даже банковские работники, обнаружив, что имеют (или могут

Видеокамера, осуществляющая снятие вводимого клиентами пин-кода, замаскированная под лоток с рекламой [95]

получить) доступ к пин-кодам клиентов, не всегда выдерживают искушение связаться с кардерами и совместно очистить клиентские счета.

В 1980-х и 1990-х была популярна установка фальшивых банкоматов и торговых терминалов. Многие из них даже выдавали клиентам деньги или товары. Ныне такие банкоматы встречаются реже.

Более распространены «приставки» к легальным банкоматам, которые незаметно для клиента считывают данные с магнитной полосы и «подсматривают» вводимый пин-код [95, 96, 97].

О распространенности подобного способа говорит то, что производители банкоматов сейчас предусматривают в картоприемнике механизм для неравномерного протягивания карты. Карта втягивается в банкомат и экстрагируется из банкомата рывками, чтобы затруднить считывание магнитной полосы возможным шпионским устройством. Впрочем, ответные технические меры уже придуманы.

Накладка на клавиатуру банкомата, снимающая вводимый пин-код [97]

Использование интернет-казино

Если бы такие казино легко и быстро выплачивали игрокам выигрыши, они были бы идеальным каналом отмывки денег для кардеров. Но в онлайновых казино легок и прост только ввод денег. А для их вывода (получения выигрыша) надо затратить немало усилий и времени; в результате далеко не факт, что игрок вообще получит свои деньги. Это не следствие жадности онлайн-казино. Это следствие действий кардеров. Если какое-либо казино начнет без формальностей выплачивать выигрыши, оно вскоре обнаружит, что кардеры составляют подавляющее большинство его игроков. От чего такое казино немедленно будет объявлено пособником со всеми вытекающими неприятными последствиями.

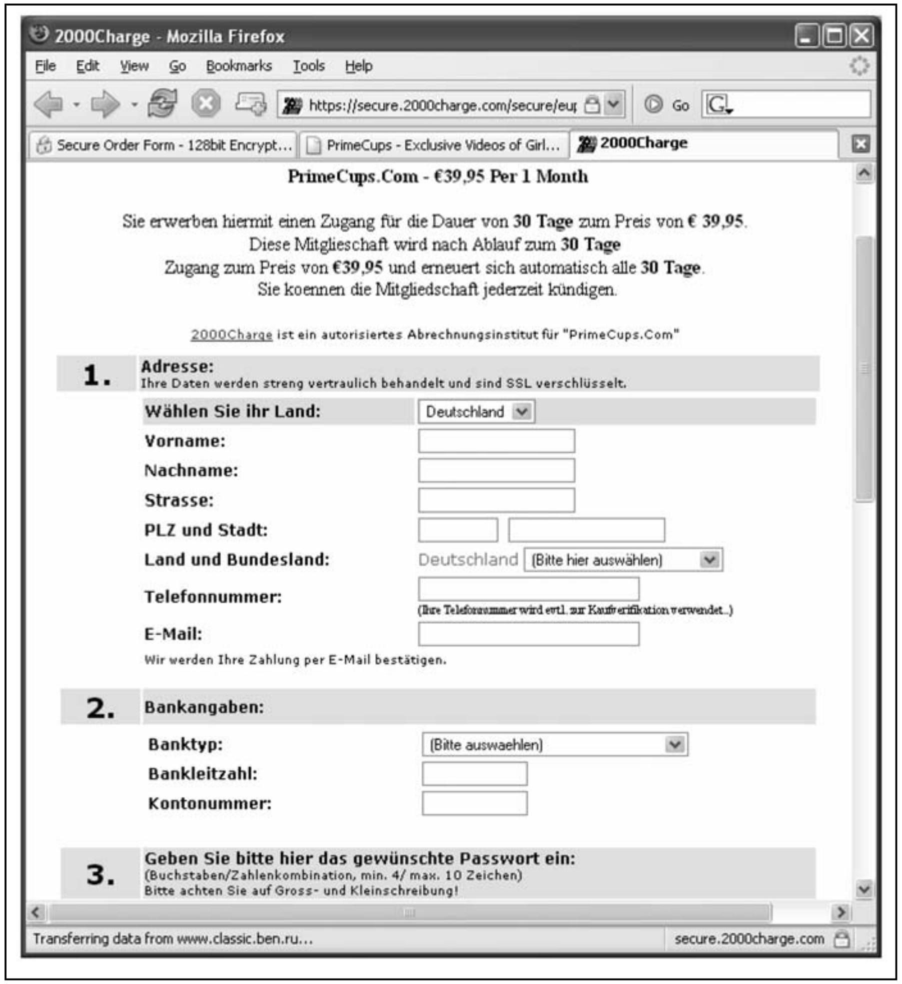
Поэтому для выплаты денег казино требует подтверждения личности игрока, а также пользуется только неанонимными системами платежей. От игрока, пожелавшего получить выплату, скорее всего, потребуют прислать скан-копию паспорта и какого-либо документа, подтверждающего место жительства, например, квитанции об оплате коммунальных услуг. Возможно, от игрока захотят получить номер телефона ради дополнительного подтверждения его личности. Выплата производится на именной банковский счет (при этом не всякий банк будет признан благонадежным) или при помощи именного чека, который отправляется по почте. В общем, онлайн-казино выработали ряд процедур, затрудняющих кардерам жизнь.

Те в ответ придумали контрмеры. Немало умельцев предлагают услуги по изготовлению скан-копий паспортов и иных документов за разумную цену ($20-40), телефонные номера в «благонадежных» странах с переводом входящих звонков на любой номер в любой стране, банковские счета, принимающие платежи, адресованные произвольным физическим лицам, и другие подобные услуги.

Также наблюдается разделение труда в области работы с самими интернет-казино. Регистрацию аккаунтов* игроков обычно поручают отдельным людям. На черном рынке кардерских товаров и услуг продаются и покупаются такие аккаунты, как пустые, так и уже «отыгранные», то есть готовые для вывода денег.

Фиктивные покупки

Типичный интернет-магазин или платный веб-сайт для получения платежей от своих клиентов использует услуги так называемого билингового предприятия – финансового учреждения, которое принимает данные банковских карт, совершает транзакции и переводит полученные деньги (за вычетом своей комиссии) на банковский счет интернет-магазина. У билинговой фирмы имеется собственная служба безопасности, препятствующая проведению мошеннических операций. Именно поэтому банки отка-



Веб-страница билинговой фирмы, на которую пользователь переадресуется со страницы платного веб-сайта для оплаты услуг при помощи банковской карты. На верху страницы мы видим наименование предприятия, в чью пользу берется платеж, и сумму

зываются работать с мелкими онлайн-магазинами напрямую и предпочитают взаимодействовать именно с билинговыми предприятиями-посредниками. Билинговое предприятие отказывает в обслуживании тем онлайновым магазинам, у которых процент отозванных транзакций (chargeback) превышает некоторый уровень, обычно 1%. Может отказать в обслуживании и по иной причине, если сочтет интернет-магазин подозрительным.

Веб-сайт типичного онлайн-магазина даже не имеет интерфейса для ввода платежных реквизитов. Посетитель веб-сайта вводит их прямо на веб-странице билинговой фирмы, естественно, пользуясь защищенным (HTTPS) соединением.

Один из способов реализации данных банковских карт состоит в сговоре между кардером и владельцем онлайнового магазина. Часто такие магазины или платные веб-сайты устраиваются специально ради приема платежей по чужим картам. Сообщники вместе пытаются обмануть билинговое предприятие, сделать так, чтобы возвратов было не больше установленного количества.

Для ввода реквизитов карт в интерфейс билинговой системы обычно нанимаются отдельные люди, набивщики. Это «чернорабочие» кардерского мира. Тем не менее от них требуется владеть определенными навыками. Набивщик должен использовать для каждой новой карты новый прокси-сервер или сокс-сервер, желательно, расположенный в той стране, в которой живет держатель карты. Он должен побеспокоиться, чтобы его компьютер соответствовал типичной конфигурации компьютера клиента.

При взаимодействии с веб-интерфейсом билинговой системы браузер пользователя сообщает следующие данные:

Система оплаты услуг без банковских карт — следствие массового кардерства

- марка и версия браузера;
- язык браузера;
- версия ОС;
- разрешение экрана;
- воспринимаемые типы данных;
- воспринимаемые языки;
- воспринимаемые кодировки данных;
- referrer, то есть адрес веб-страницы, с которой пользователь перешел на данную веб-страницу;
- некоторые другие настройки.

Понятно, что если во время такого взаимодействия передаются реквизиты банковской карты Джона Смита из США, а язык браузера выставлен украинский, то система заподозрит неладное. Также возникнет подозрение, если с одного и того же IP-адреса будут введены карточные реквизиты двух разных людей из разных стран.

Поэтому набивщики получают необходимые инструкции и, если надо, ПО для своей работы.

Именно из-за нашествия кардеров стали появляться альтернативные системы оплаты услуг в Интернете. Некоторые платные веб-сайты уже не принимают банковских карт. Оплата производится через телефонный звонок по платной линии или иным подобным способом. У таких способов больше накладные расходы, но это дешевле, чем постоянно решать проблемы, создаваемые из-за кардинга.

Реальный пластик

На кардерском жаргоне «реальным пластиком» именуются полноценные твердые копии банковских карт. На них должен присутствовать цветной рисунок, голограмма, иметься эмбоссированное (выдавленное) имя держателя и магнитная полоса с нужными данными.

Для этого способа реализации требуется дамп* карты. Пин-код не нужен. По дампу изготавливается твердая копия карты. Она должна не только нести верные данные на магнитной полосе, но и выглядеть соответственно. Рисунок карты, конечно, не обязан совпадать с оригинальным, но он должен присутствовать и быть хорошего качества: не смазываться, не отслаиваться. Желательно, чтобы название банка и карты соответствовало коду (первые 6 цифр номера карты); впрочем, продавцы редко обращают на это внимание.

К такой поддельной карте реализатору желательно иметь поддельный документ. Продавец или кассир не обязан спрашивать у покупателя удостоверение личности, но может это сделать, если возникнут подозрения. А они, скорее всего, возникнут, поскольку кардер с «реальным пластиком» пойдет покупать не корзинку продуктов в супермаркете, а что-нибудь по-

дороже, что можно будет перепродать хотя бы за 40-50% стоимости. Совершить много покупок по поддельной карте не удастся, одна, две, может быть, три – и держатель карты спохватится и заблокирует ее.

Бывает, что фальшивый документ изготавливают на имя держателя карты. Это надежнее, но дороже. Ведь поддельная карта может быть использована не более 2-3 раз. После этого она в лучшем случае будет заблокирована, а в худшем – попадет в стоп-лист. Соответственно, и поддельный документ нужно будет выбросить вместе с картой. Другой вариант – «постоянный» документ, вместе с которым можно использовать несколько разных карт. В соответствии с именем в документе наносится (эмбоссируется) имя на карте. То есть имя на карте будет соответствовать документу, но не будет соответствовать имени на магнитной полосе. В этом случае затраты ниже, но выше риск, поскольку продавец может сравнить имя на чеке и имя на карте.

Образец же подписи на поддельной карте можно нарисовать такой, какой удобно.

Пластиковые заготовки для банковских карт, оборудование для нанесения изображений, эмбоссирования и записи магнитной полосы имеется в свободной продаже. Но приобретать его целесообразно, только если собираешься изготавливать карты сотнями. Единичные экземпляры выгоднее заказывать на стороне. Полное изготовление банковской карты на черном рынке обойдется в 100-200 долларов.

Белый пластик

Карта, имеющая только записанную магнитную полосу, именуется у кардеров «белым пластиком». Ее изготовление обходится совсем недорого. Однако область использования ограничена лишь банкоматами. Разумеется, необходимо знать пин-код.

Набор дамп карты + пин-код сто́ит на черном рынке дорого, зато с его помощью можно выжать карточный счет досуха, сняв в банкомате весь остаток и весь кредитный лимит.

Заготовки для банковских карт

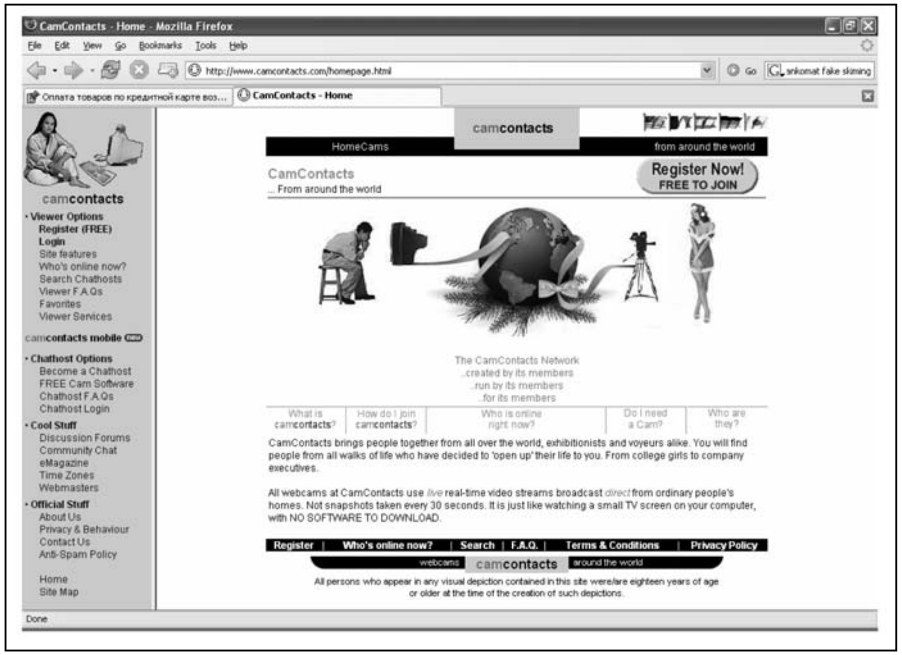
Многие банки ставят ограничения для банкоматных транзакций – по географии, по максимальной сумме за раз и по максимальной сумме за день. Это несколько усложняет кардерам жизнь. Карту могут успеть заблокировать и занести в стоп-лист, пока еще не все деньги с нее сняты.

Кроме реализации в банкоматах возможны варианты покупки товаров по «белому пластику» в магазинах. Естественно, лишь по сговору с продавцом.

Посреднические онлайн-сервисы

Инструментом кардера может стать почти любой интернет-сервис, где предусмотрена выплата денег клиентам.

Некоторое распространение имеют посреднические сервисы по обмену видео. Суть их состоит в том, что одни пользователи желают транслировать видеоизображение через Интернет, а другие желают его потреблять. (Разумеется, как правило, речь идет об эротическом видео, но посредник предпочитает об этом «не знать».) Посредник организует этот процесс, сводит покупателя с продавцом и осуществляет расчет между ними. Себе берет процент за посредничество.



Один из многочисленных сайтов, предлагающих посредничество в продаже онлайн-видео. Такие сайты привлекательны для кардеров в качестве метода обналичивания

Поскольку от покупателей принимаются платежи по банковским картам, а выплаты продавцам производятся чеком или банковским переводом, есть возможность «отмывания». Кардер регистрируется на таком посредническом сайте как покупатель, как продавец и начинает продавать услуги самому себе.

Это также не простой путь. Службы безопасности знают, как притягательны для кардеров подобные сервисы, и всячески стараются воспрепятствовать. Выплаты обставляются различными условиями наподобие интернет-казино. Кардеры, разумеется, находят ответные меры.

Почему мошенничество?

В заключение несколько слов о квалификации кардерских действий.

В УК РФ имеется специальная статья 187, на первый взгляд, специально ориентированная на кардеров: «изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов». Но диспозиция статьи сформулирована без учета сегодняшних технологий кардинга. Юристы расходятся во мнении, что считать «сбытом» банковской (расчетной) карты. Одни юристы [20] утверждают, что сбытом можно считать лишь действия, предполагающие переход карты (как вещи) к иному владельцу. При таком подходе привлечь к уголовной ответственности по этой статье можно только одного члена преступной группы – того, который непосредственно печатает твердые копии карт, да и то лишь в том случае, если расплачивается ими не сам. Другие юристы [W04] полагают, что «сбыт» состоит также в использовании поддельной карты в качестве средства платежа. Но и в том, и в другом случае из этого состава выпадает использование лишь данных банковских карт, без изготовления твердых копий, а ведь эти случаи составляют большинство.

Законодательство здесь сильно отстало от развития технологий. Впрочем, вряд ли стоит его «подтягивать». Платежные системы активно переходят от карт с магнитной полосой к чиповым картам. Для новой технологии и методы мошенничества будут новыми.

Для всех кардерских действий, которые сводятся к получению денег или материальных ценностей, годится статья 159 УК «мошенничество». Те случаи, когда с помощью чужой карты приобретается не имущество, а услуга, можно также квалифицировать как мошенничество в отношении держателя карты, если деньги были списаны. А если не списаны, то подойдет статья 165 УК «причинение имущественного ущерба путем обмана или злоупотребления доверием».

Мошенничество с трафиком

Автоматизированные системы расчетов (билинговые системы), а также средства сбора данных для таких систем (предбилинг, mediation) операторов связи всегда являлись объектом интереса мошенников, казнокрадов и прочих криминальных элементов. Изменив данные в биллинговой системе, можно осуществить мошенничество, хищение, растрату на значительную сумму. Сложность таких систем велика, доступ к ним имеют сразу многие лица из персонала и даже клиентов предприятия, поэтому всегда имеется достаточно технических возможностей получить доступ и изменить данные.

Мошенничество с данными билинга достаточно распространено. Оно распространено настолько, что существуют нормативы списания средств на такие злоупотребления. На рынке есть особые программные продукты для выявления и пресечения подобного рода действий, они именуются «fraud management systems». Само название свидетельствует о том, что речь идет не о предотвращении мошенничества вовсе, а лишь о разумном снижении убытков от такого мошенничества.

Расследование подобных преступлений требует специальных знаний в двух областях. Во-первых, в области бизнеса отрасли связи. Порядок пропуска трафика, его техническая организация, взаиморасчеты между операторами, особенности тарифов – все это область специальных знаний. Во-вторых, требуются знания в области ИТ, поскольку все билинговые системы – это компьютерные информационные системы, и организация несанкционированного доступа к ним является предметом соответствующих специальных знаний.

Автору неизвестны случаи, когда мошенничество с трафиком было совершено «снаружи», то есть без содействия сотрудника пострадавшей компании либо сотрудника иного оператора связи. Теоретически такие случаи возможны, но на практике они, видимо, очень редки.

Есть две типичные схемы подобного мошенничества. В первом случае сотрудник оператора связи вступает в сговор с ее клиентом (или несколькими клиентами) и тем или иным способом изменяет данные об оказанных услугах (объеме, времени, тарифах). Во втором случае «выгодоприобретателем» от мошенничества выступает другой оператор связи, который получает незаконный доход или экономию за счет манипуляций с тарифами, типом трафика и т.п. В этом случае сговор с сотрудником пострадавшего оператора не обязателен, хотя и желателен.

Следует заметить, что деяние, называемое «мошенничеством с трафиком», не всегда является правонарушением. Иногда это всего лишь нарушение условий межоператорского договора. А иной раз – и вовсе правомерная оптимизация затрат при помощи, например, альтернативных путей пропуска трафика.

Нарушение авторских прав в офлайне

Способ

Обсуждаемое преступление соответствует частям 2 и 3 ст. 146 УК. В данной главе речь идет лишь о тех случаях, когда распространение произведения происходит не через сеть, а в офлайне* – путем передачи (продажи) носителя или путем инсталляции с такого носителя.

Распространенностью этого состава в российской криминальной статистике мы обязаны легкости его раскрытия. Торговля на улицах контрафактными дисками и обилие рекламы услуг «черных инсталляторов» позволяет обнаружить и раскрыть такое преступление очень быстро, в любой день, когда возникнет желание.

Объявления «черных инсталляторов»

Преступник

Подозреваемый в большинстве случаев известен, поскольку задерживается на месте после проведения проверочной закупки.

В некоторых случаях преступником является не непосредственный продавец, а директор или товаровед магазина, выставивший в продажу контрафактные экземпляры. Хотя чаще хитрый директор фирмы, прекрасно зная о контрафактности реализуемых программ, делает крайним продавца или инсталлятора.

Потерпевший

Потерпевшим является правообладатель. Большинство правообладателей на популярные продукты – зарубежные. Не все они имеют представительства в России. Не все из них охотно соглашаются выступать потерпевшими.

Российские правообладатели также не всегда соглашаются писать заявление о возбуждении уголовного дела.

По части 2 ст. 146 возбудить дело можно только по заявлению правообладателя. Без такого заявления возбудить дело можно лишь по части 3 этой статьи – при особо крупном размере, более 250 000 рублей.

Для установления принадлежности авторских прав на то или иное произведение часто назначается автороведческая экспертиза. На разрешение эксперту ставится следующий вопрос: кто является вероятным правообладателем для представленного произведения (фонограммы, фильма, программы для ЭВМ)? Или в такой формулировке: какие имеются признаки на экземпляре произведения, указывающие на принадлежность авторских прав на это произведение? Автор полагает, что подобную экспертизу правильнее называть не автороведческой, а компьютерно-технической или программно-технической.

Вывод эксперта об авторе и правообладателе может носить лишь предположительный характер. То, что данное лицо является правообладателем на данное произведение, – это факт юридический, а не технический. Исключительные права на произведение могут быть переданы по договору другому лицу, но произведение от этого не изменится ни на бит. Эксперт лишь ищет на экземпляре произведения какие-либо указания на правообладателя, уведомления об авторских правах, которые принято там ставить. А строго установить правообладателя – это задача следователя. Принадлежность исключительных прав на произведение устанавливается документами – авторским договором, договором об уступке исключительных прав, свидетельством о регистрации прав на продукт и т.д.

В некоторых случаях правообладатели делегируют некоторые свои полномочия ассоциациям, занимающимся защитой интеллектуальной

собственности на коллективной основе. Такая ассоциация может считаться законным представителем потерпевшего. Для этого она должна представить соответствующий договор.

Следы

Из следов технического характера здесь присутствует разве что установленное «черным инсталлятором» программное обеспечение. Соответствующий носитель следует отправить на экспертизу для установления состава установленного ПО и его вероятного правообладателя.

Автор еще раз хотел бы здесь подчеркнуть, что установление контрафактности программного обеспечения (будь оно в виде развертки на жестком диске или в виде дистрибутива на пиратском CD) не может являться предметом программно-технической экспертизы. Равно как и любой другой экспертизы. Контрафактность – это вопрос правоотношений между правообладателем и пользователем: заключен ли авторский договор, уплачены ли деньги, соблюдены ли условия договора (лицензии). Исследованием экземпляра самóй программы этих обстоятельств установить невозможно. Программно-техническая экспертиза может лишь выявить признаки контрафактности, которые сами по себе ничего не доказывают и могут служить лишь косвенным доказательством. Это обстоятельство подтверждено постановлением Верховного суда [L02]: «Понятие контрафактности экземпляров произведений и (или) фонограмм является юридическим. Поэтому вопрос о контрафактности экземпляров произведений или фонограмм не может ставиться перед экспертом».

Также не может быть предметом КТЭ установление стоимости экземпляров ПО. Стоимость устанавливается товароведческой или экономической экспертизой, либо принимается равной цене этого ПО, если оно продается за одинаковую цену всем потребителям (подробнее об этом – в главе «Стоимость ПО» раздела 5).

Часто для установления стоимости экземпляров ПО или прав на его использование пользуются данными, которые представлены потерпевшим, например, его официальным прайс-листом. Это неправильно. Программное обеспечение, в отличие от иного рода товаров, может продаваться за существенно разную цену. Разница в цене в 3-5 раз на одну и ту же программу для разных классов потребителей является на рынке ПО обычным делом.

К тому же более ранние версии ПО после выхода более свежих версий обычно снимаются с продажи совсем. Стоимость версии, которая на момент совершения преступления не продавалась, не может быть приравнена к стоимости более свежей версии. При обновлении расширяется функциональность ПО, исправляются ошибки, улучшается дизайн и иные потребительские свойства продукта. Поэтому стоимости новой и

старой версии не могут быть равны. Некоторые производители даже готовы передавать пользователям право на использование устаревших версий бесплатно или за символическую цену. Для определения стоимости версии ПО, изъятой из продажи, необходимо назначать экономическую или товароведческую экспертизу. В ней желательно участие не только экономиста, но и специалиста по ИТ или программированию – для учета специфики такого товара, как ПО.

Политизированность

Общественная опасность нарушений авторских и смежных прав ныне оценивается как достаточно высокая. Во всех странах заметна тенденция к ужесточению наказаний за такие нарушения, и следовательно, к повышению оценки их общественной опасности. Не секрет, что указанное ужесточение в большинстве стран проводится под давлением США, на территории которых сосредоточено большинство крупных правообладателей и экономика которых сильно зависит от соответствующих доходов. С макроэкономической точки зрения массовое нарушение авторских прав сводится к перераспределению доходов между более развитыми и менее развитыми странами. И размер этих доходов достаточно велик, чтобы существенно влиять на благополучие экономики в целом. Поэтому вопрос об авторских правах, а также иных правах интеллектуальной собственности – это вопрос политический. Политизированность неизбежно влияет на организацию раскрытия и расследования таких дел.

С одной стороны, это означает, что борьба с нарушениями авторских прав, ее размер, интенсивность и направленность регулируются высшим государственным руководством. Отсутствие такой борьбы отрицательно повлияет на отношение со стороны развитых стран, где расположено большинство правообладателей. Другая крайность – излишне рьяная борьба с нарушениями авторских и смежных прав – может нанести ущерб национальной экономике из-за сильного увеличения платежей иностранным правообладателям или невозможности пользоваться высокотехнологичной продукцией.

С другой стороны, политические партии и общественные деятели не могут не уделять внимания вопросам авторских прав и соответствующим нарушениям. В зависимости от своих позиций они склонны по-разному освещать события, лоббировать решения, использовать уголовные и гражданские дела, связанные с авторскими правами, в пропагандистских целях.

Понятно, что большинству сотрудников правоохранительных органов не нравится роль инструмента в этой политической и идеологической борьбе. Поэтому они предпочитают в делах, связанных с авторскими правами, воздерживаться от проявления инициативы, а лишь исполнять «от сих до сих» полученные сверху указания.

Нарушение авторских прав в Сети

Способ

Неправомерное воспроизведение охраняемых произведений в онлайне* осуществляется путем размещения их на общедоступных веб-серверах, FTP-серверах или в файлообменных сетях*.

Хотя заголовок говорит лишь об авторских правах, на самом деле все нижесказанное относится и к иным правам интеллектуальной собственности – смежным правам, патентным правам, правам на товарные знаки и т.п.

«Размещение на общедоступных серверах» – это нестрогое выражение. Конкретное правомочие, которое подозреваемый осуществляет, не имея на то разрешения, сформулировано так: «Сообщать произведение таким образом, при котором любое лицо может иметь доступ к нему в интерактивном режиме из любого места и в любое время по своему выбору (право на доведение до всеобщего сведения)» – абзац одиннадцатый пункта 2 статьи 16 Закона РФ «Об авторском праве...». Это правомочие было специально внесено в закон в 2004 году для учета тех случаев, когда произведение распространяется через веб-сайт или FTP-сайт.

Иногда произведение размещается не в глобальной компьютерной сети, а в локальной. При этом варианте качественных отличий нет, если только круг пользователей локальной сети не ограничивается одной семьей. Все, что превышает этот круг, уже не может считаться «для личного пользования». Большую популярность имеют так называемые домовые сети, охватывающие подъезд, жилой дом или пару домов. Там часто встречаются сервера, содержащие большое количество музыки, фильмов и программного обеспечения.

Преступник

Размещением контрафакта в Сети обычно занимаются не из корыстных побуждений. В большинстве случаев правонарушитель действует, либо вообще не задумываясь о противоправности, либо руководствуясь нонконформизмом.

Случаи корыстной мотивации, пожалуй, исчерпываются получением дохода от рекламы, которая размещена на веб-сайте, содержащем популярный, но контрафактный контент (так называемый варез*). Веб-мастер обычно получает доход со своего веб-сайта через размещение на нем рекламы. Доход тем больше, чем выше посещаемость ресурса. Разместить на сайте популярный варез – верный путь быстро поднять посещаемость. Многие так и поступают, либо не задумываясь о нарушении прав, либо надеясь на «авось пронесет».

Потерпевший

Контрафактных произведений в Сети такое количество, что правоохранительные органы не занимаются этими правонарушениями в инициативном порядке. Инициатором всегда выступает потерпевший.

Потерпевшим может быть как сам правообладатель, так и организация по коллективному управлению авторскими и смежными правами или общественная организация-объединение правообладателей. В последнем случае должен быть представлен договор, в котором правообладатель уполномочивает такую организацию представлять свои интересы в случае нарушения авторских прав.

Подобные организации бывают чрезвычайно активны и настойчивы. Но иногда они заинтересованы вовсе не в уголовном преследовании виновного, а всего лишь в прекращении распространения по Интернету защищаемого произведения. После того, как контрафактная программа или иное произведение убрано с сайта, заявитель может потерять к делу всякий интерес и прекратить сотрудничество с правоохранительными органами.

Бывает и другая крайность, когда организация, защищающая авторские права своих членов, предоставляет правоохранительным органам не только информацию об обнаруженном нарушении, но и протокол осмотра и заключение своего эксперта о контрафактности. Понятно, что к доказательствам, которые собраны заинтересованной стороной, надо относиться критически, а заключение эксперта, который находится в служебной или иной зависимости от потерпевшего (представителя потерпевшего), вообще не может быть признано доказательством в силу УПК. Но иногда следователь, чтобы уменьшить себе работу, идет на поводу у представителя потерпевшего и фактически строит дело только на полученных от него документах. Автор неоднократно сталкивался с такой практикой и, конечно же, считает ее недопустимой.

В качестве примера можно привести Некоммерческое партнерство поставщиков программных продуктов (НП ППП) – организацию, созданную российскими правообладателями и ведущую работу по защите их авторских и смежных прав. Такая работа, безусловно, полезна. Но следует помнить, что указанное партнерство фактически является заинтересованным лицом, хотя формально не выступает в качестве потерпевшего или представителя потерпевшего в конкретном уголовном деле. Поэтому эксперты, предоставленные этой организацией, не могут считаться независимыми, если только потерпевший входит в число членов НП ППП. То же относится к разработанной ими методике проведения экспертиз [94] и к регулярно публикуемым каталогам цен на программные продукты – все эти материалы следует рассматривать наравне с материалами, предоставленными потерпевшим, то есть заинтересованной стороной.

Следы

При доведении до всеобщего сведения образуются такие следы технического характера:

- записи в логах веб- или FTP-сервера при записи файлов на сервер (upload);
- записи в логах веб- или FTP-сервера при получении файлов потребителями – свидетельствует об интерактивной доступности файлов иным лицам;
- следы на компьютере, с которого подозреваемый записывал файлы на общедоступный сервер, локальные копии этих файлов;
- архивы и логи сообщений электронной почты и ICQ, в которых подозреваемый сообщал другим пользователям о доступности файлов по определенному сетевому адресу.

Кроме того, подозреваемый может иметь договор с оператором связи, на ресурсе которого производилось размещение произведения.

Фишинг

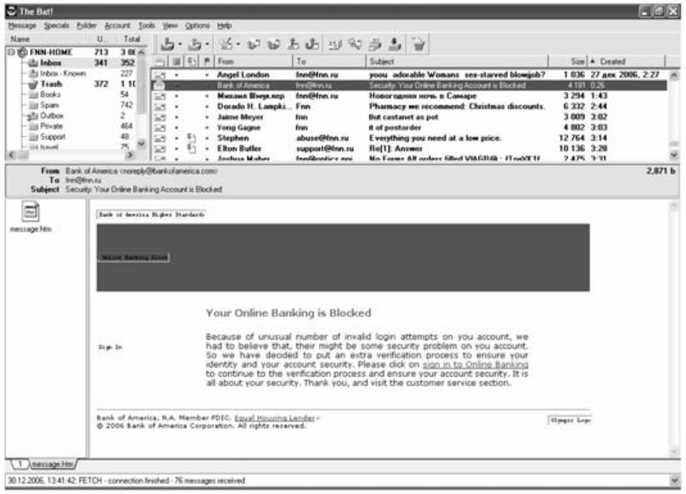
Способ

Фишинг (phishing) – это выманивание у потерпевших их конфиденциальных данных методами социальной инженерии. Как правило, речь идет о номерах банковских карт, их пин-кодах, паролях к системе управления банковским счетом (онлайн-банкинг) и другой информации, которую можно потом обратить в деньги. Наибольшей популярностью у фишеров пользуются самые распространенные банки и платежные системы: «Citi bank» «eBay» и «PayPal».

Выманивание данных происходит при помощи подложных сообщений электронной почты и/или подложных веб-сайтов. Как правило, пользователя стараются напугать, например, закрытием его счета или приостановкой оказания услуг, если он не выполнит предложенную мошенником процедуру. Часто, если не всегда, ссылаются на якобы произошедшую аварию, утрату аутентификационных данных, иные чрезвычайные обстоятельства, даже на действия мошенников-фишеров.

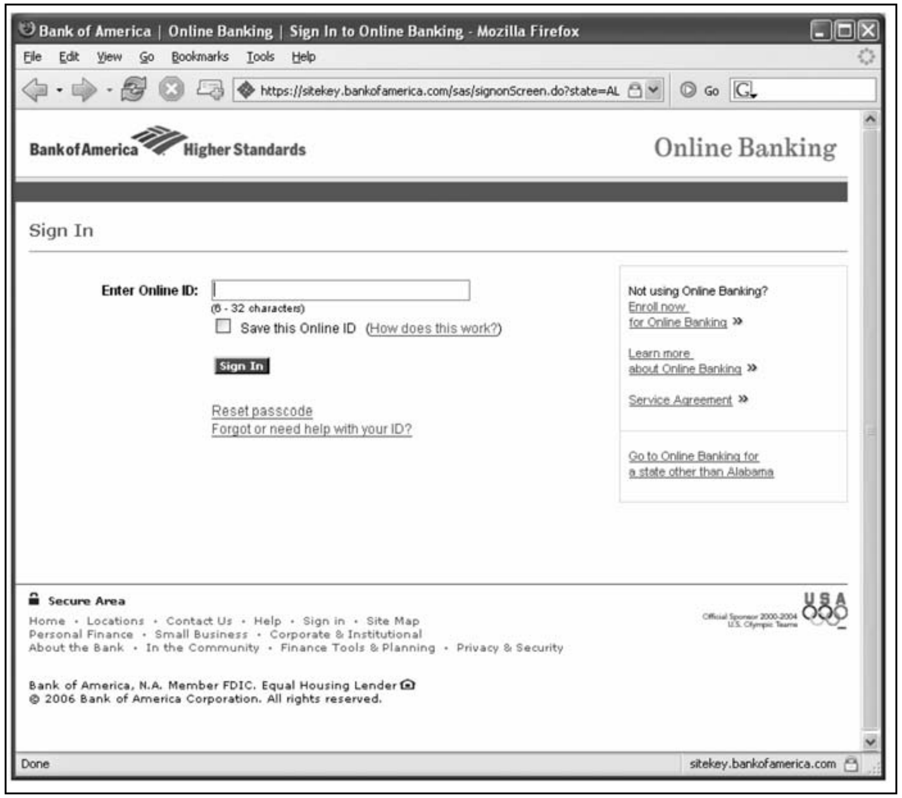
Хотя вероятность обмануть каждого адресата невелика, но за счет массовой рассылки и охвата огромной аудитории фишерам удается собрать некоторое количество ценных сведений с каждой рассылки. Фишинг стал экономически выгоден лишь после появления дешевых технологий спам-рассылки.

Фишинг после своего возникновения стал необычайно популярен среди мошенников. Исследователи отмечают [73, W05] его высокую доходность, изощренность, глобальность, возможность и выгодность его использования против клиентов самых разнообразных банковских, платежных и даже некоммерческих систем.



Типичное фишинговое письмо о якобы заблокированном аккаунте в системе управления банковским счетом (онлайн-банкинг). Ссылка ведет на подложный сайт, где пользователю будет предложено ввести свои конфиденциальные данные. Ссылка http://sigotama.com/www.bankofamerica.com/BOA/sslencrypt218bit/online_banking/index.htm лишь слегка похожа на настоящий адрес банка – www.bankofamerica.com

Фишинговый веб-сайт, копирующий страницу авторизации подлинного веб-сайта



Для сравнения – подлинная страница авторизации банка. Обратите внимание на защищенный режим соединения (HTTPS), фишерский же сайт использует протокол HTTP, без шифрования и аутентификации

Логотипы банков и платежных систем, их веб-сайты подделываются с максимально возможной точностью. Чтобы ввести жертву в заблуждение, мошенники различными способами маскируют URL своего сайта, делая его максимально похожим на подлинный URL. Часто для этого регистрируется новый домен для каждой новой рассылки. Подложные ссылки маскируются и иными способами.

Вот еще пример фишингового письма.

Письмо фишера. Видимый текст на самом деле является графическим вложением. С этой картинки поставлена гиперссылка на подложный сайт

Естественно, видимая гиперссылка ведет не на указанный сайт, а на другой, подложный, URL которого виден из исходного текста сообщения.

Исходный код сообщения:

```
...
From: «Fifth Third Bank» <customerservice-num74936499573ver@securi-
ty.53.com>
To: «Abuse» <abuse@wimax.ru>
X-Virus-Scanned: Norton
User-Agent: MIME-tools 5.503 (Entity 5.501)
X-Mailer: MIME-tools 5.503 (Entity 5.501)
X-Priority: 3 (Normal)
MIME-Version: 1.0
```

```
Content-Type: multipart/related;
 boundary="WO1_WNI98HTQGVW7PI"
Date: Thu, 11 Jan 2007 11:57:32 +0300
X-Original-Message-ID: <auto-000001001154@mail1.wimax.ru>
Subject: [ABUSE]Fifth Third Bank - we need to update your informa-
tion!
 -Thu, 11 Jan 2007 03:57:25 -0500
Status: R
X-Status: NT
X-KMail-EncryptionState:
X-KMail-SignatureState:
X-KMail-MDN-Sent:


--WO1_WNI98HTQGVW7PI
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=utf-8">
<META content="MSHTML 6.00.2800.1522» name=GENERATOR></HEAD>
<BODY bgcolor="#FFFFF7» text="#A7DF6E">
<a HreF=http://www.53.com.bankingportal.id1568110.gdotbotns.net/conf>
<img src="cid:JI4UU2RCCX» border=0></a>
</p><p><font color="#FFFFF1">Send an ambulance. boor autobiography
She had taken the time to interlace its stout steel loops with
barbed wire.</font></p><p><font color="#FFFFF0">He had tried stand-
ing on the right leg and had found he could, for short times, but
doing so produced a low, primal agony that lasted for hours. He and
his first wife had honeymooned on Maui. I said I didn't call looking
at things in my own house snooping. You've been working so hard. The
bag won't be zipped. The letter was an exhaustive (and ultimately
exhausting) manual of where Mrs Roman D. You see, I began by loving
only the part of you that makes such wonderful stories, because
that's the only part I had?? the rest of you I didn't know anything
about, and I thought that part might really be quite unpleasant.
colloq</font></p>
</BODY>
</HTML>

--WO1_WNI98HTQGVW7PI
Content-Type: image/gif; name="cater.gif"
Content-Transfer-Encoding: base64
Content-ID: <JI4UU2RCCX>
```


```
R0lGODlhWAJ9AfXJAPv4/9ENDfb2+u/v9dTU1JycnZOTk4+PkfPz8+Pj49fX2cPDw3t7f
GNjY+vr69vb3M/P0MzMzLy8vLe3uKysrKOjo4uLjBQanLOzs4KCgnV1dWxsbF1dXVVVVU
xMTENDQzs7OzQ0NCsrKyIi
IhwcHBMTEwAAAAAAAAAAAAAAAAAA
...
```


Посмотрим на сведения о домене, на котором живет фишерский сайт:

```
$>whois gdotbotns.net

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.inter-
nic.net
for detailed information.


 Domain Name: GDOTBOTNS.NET
 Registrar: REGISTER.COM, INC.
 Whois Server: whois.register.com
 Referral URL: http://www.register.com
 Name Server: NS1.DOTORB.NET
 Name Server: NS1.IGARNS.NET
 Name Server: Q1.OXIDIZER-NS.NET
 Status: clientDeleteProhibited
 Status: clientTransferProhibited
 Updated Date: 10-jan-2007
 Creation Date: 08-jan-2007
 Expiration Date: 08-jan-2008

>>> Last update of whois database: Thu, 11 Jan 2007 07:48:22 EST <<<

...
Registration Service Provided By: GotNameDomains.com
Contact: gmgr@gotnamedomains.com

Domain name: gdotbotns.net

Administrative Contact:
 5920 St
 Marie Domzalski (ra50sso50n@yahoo.com)
 +1.2152881490
 Fax: -
 3546 Belgrade St.
 Philadelphia, PW 19134
 US

Technical Contact:
 5920 St
 Marie Domzalski (ra50sso50n@yahoo.com)
 +1.2152881490
 Fax: -
 3546 Belgrade St.
 Philadelphia, PW 19134
 US

Registrant Contact:
```

```
 5920 St
 Marie Domzalski (ra50sso50n@yahoo.com)
 +1.2152881490
 Fax: -
 3546 Belgrade St.
 Philadelphia, PW 19134
 US

Status: Locked

Name Servers:
 ns1.dotorb.net
 ns1.igarns.net
 q1.oxidizer-ns.net

Creation date: 08 Jan 2007 21:05:18
Expiration date: 08 Jan 2008 21:05:18
...
```

Как видно, доменное имя активировано в тот же день, когда производилась рассылка, а зарегистрировано за два дня до того. Надо ли говорить, что указанный в реестре почтовый адрес владельца домена (Белградская улица, город Филадельфия, США) не существует?

Вишинг (vishing) аналогичен фишингу. Только вместо направления жертвы на подложный сайт ее просят позвонить по подложному телефонному номеру, который якобы принадлежит банку или другой доверяемой инстанции. В телефонном разговоре (или при автоматизированном общении с использованием тонального набора) у жертвы выманивают конфиденциальную информацию.

В условиях массового перехода на IP-телефонию несложно получить в пользование анонимный трудно отслеживаемый номер телефона. Имеется также возможность перехватить вызовы на чужой номер, то есть на подлинный номер банка.

Фарминг – разновидность фишинга. Отличие в том, что подлинный ресурс (обычно веб-сайт банка) подменяется на подложный не методами социальной инженерии, а число техническими методами – при помощи атаки на DNS, внедрения пользователю вредоносной программы и т.п.

Выманивание персональных данных можно производить и более изощренным способом. Например, злоумышленник создает развлекательный ресурс. При регистрации на этом ресурсе от пользователя требуется сообщить свой адрес электронной почты, а также выбрать пароль. С некоторой вероятностью пользователь использует тот же пароль, что и для своего почтового аккаунта. Это даст возможность злоумышленнику просматривать электронную почту жертвы, в которой могут попасться конфиденциальные данные.

Преступник

Фишинг и реализация его результатов не под силу одному человеку. Этим занимаются преступные группы, состоящие как минимум из двух членов. Первый сообщник или группа сообщников занимается выманиванием конфиденциальных данных, которые передаются или продаются второму сообщнику или группе сообщников для реализации.

Вероятный тип преступника – «е-бизнесмен» (см. главу «Личность вероятного преступника»).

Потерпевший

Сами фишерские уловки рассчитаны на людей неосведомленных, не сведущих в информационных технологиях и невнимательно относящихся к предупреждениям банков, платежных систем и других инстанций. Таковых – большинство.

Одна из онлайновых антифишинговых служб – «RSA FraudAction», бывшая «Cyota»

Установить потерпевших, которые сами не обратились в правоохранительные органы, можно следующими способами:

- проверить обращения в банк или иное предприятие, на клиентов которого было рассчитано мошенничество, – большинство обманутых не считают нужным обращаться в правоохранительные органы или думают, что произошло не мошенничество, а ошибка в расчетах, они вместо этого обращаются в банк;
- если есть доступ к статистике трафика или логам фишерского веб-сайта, можно установить и проверить всех пользователей, обращавшихся к этому сайту (конечно, не все из них стали жертвами мошенничества, но значительная часть);
- при помощи клиентской службы банка или самостоятельно разослать всем клиентам банка уведомления об имевших место попытках мошенничества с просьбой проверить свои счета и с обещанием вернуть украденные деньги.

Банк или платежная система также могут выступать в качестве потерпевшего по делу о фишинге. Могут, но не всегда желают, поскольку такой процесс отрицательно сказывается на деловой репутации. Однако они всегда заинтересованы в предотвращении дальнейших мошеннических действий против своих клиентов. Многие банки и платежные системы сами занимаются отслеживанием деятельности фишеров или поручают это специальным агентствам. Накопленной информацией о деятельности фишеров они с удовольствием поделятся с правоохранительными органами.

Киберсквоттинг

Определение

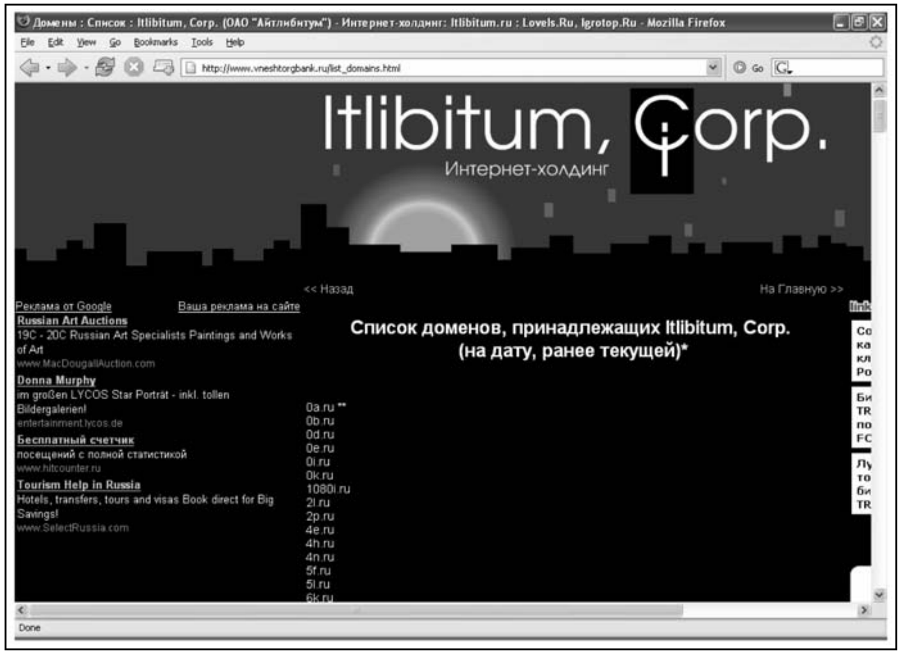
Этим термином именуется приобретение доменного имени с целью его недобросовестного использования либо с целью не допустить его добросовестного использования другим лицом.

Доменное имя в подавляющем большинстве стран является объектом купли-продажи, и стоимость его может существенно возрастать в зависимости от разных факторов.

Сразу после появления доменных имен, в 1980-х, они не имели коммерческой ценности. Но с развитием так называемого «е-бизнеса», во второй половине 1990-х годов, стало ясно, что хорошее доменное имя дает существенную прибавку числа клиентов. Следовательно, доменное имя имеет стоимость, является активом компании, может покупаться и продаваться. По данным компании «comScore Networks», в 2006 году объем розничных продаж через Интернет в США превысил 100 млрд. долларов. В странах Евросоюза в этом же году объем продаж составил около

130 млрд. Оценочная стоимость самых популярных доменных имен достигает десятков миллионов долларов. Зафиксированы реальные сделки с доменными именами на суммы в несколько миллионов.

Естественно, в таких условиях появляются желающие заработать на перепродаже доменных имен – киберсквоттеры.



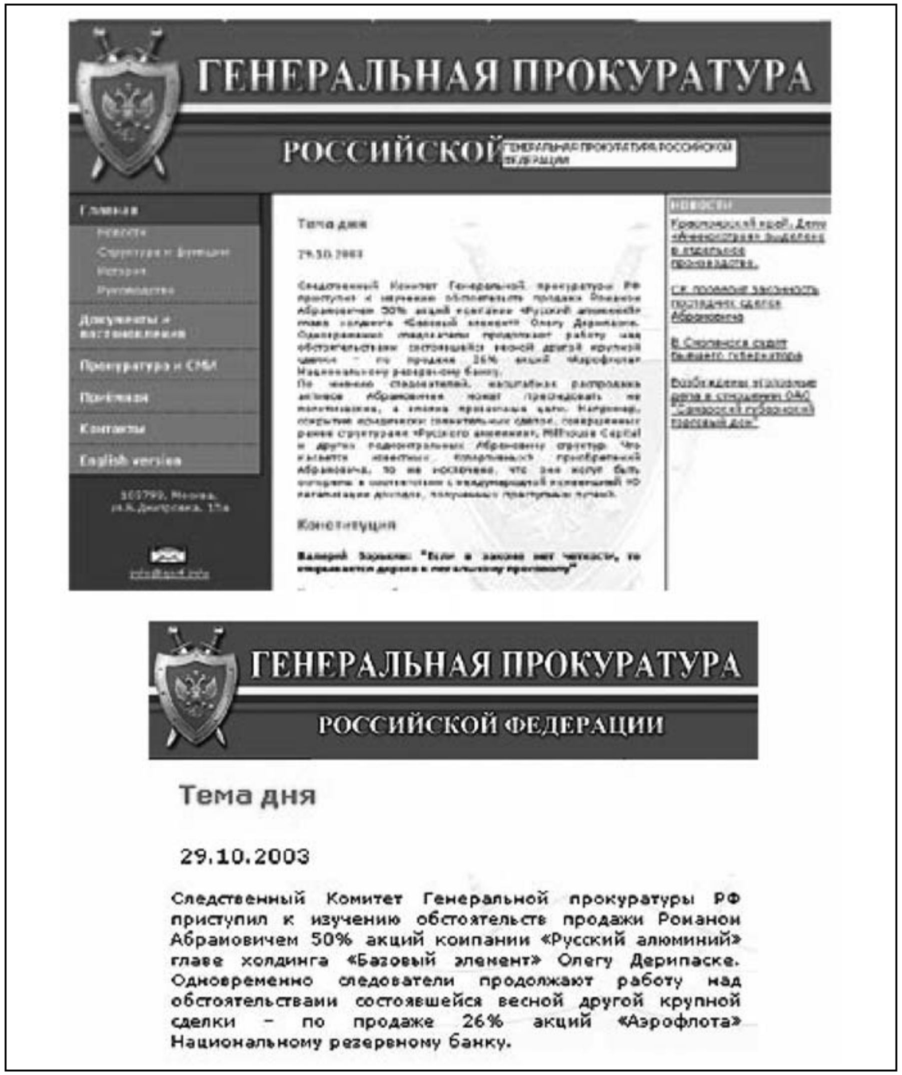
При запросе веб-сайта www.vneshtorgbank.ru мы попадаем не на сайт банка, а на страницу киберсквоттера, который предлагает к продаже это имя и еще много других имен – всего в списке 490 доменов

Правовая оценка

Далеко не всегда киберсквоттинг криминален. Сам по себе захват доменного имени преступлением не является. Даже когда он производится в целях недобросовестной конкуренции, это нарушение рассматривается в гражданском порядке или по внесудебной процедуре, установленной регистратором.

Уголовное преступление совершается тогда, когда на основе киберсквоттинга происходит вымогательство (ст. 163 УК), мошенничество (ст. 159 УК) или принуждение к совершению сделки (ст. 179 УК). Изредка возможны и некоторые другие виды преступлений – обман потребителей, уклонение от уплаты налогов и т.д.

Большинство случаев киберсквоттинга не попадают в сферу уголовных преступлений. Захват домена с целью продажи или воспрепятствования его использованию может являться нарушением прав на товарный знак или иное средство индивидуализации, актом недобросовестной конкуренции, иным злоупотреблением правом, наносящим ущерб. Во всех подобных случаях заявитель отсылается к гражданскому порядку разрешения споров.



Фрагменты фальшивого сайта Генпрокуратуры gprf.info

О вымогательстве можно вести речь лишь тогда, когда киберсквоттер угрожает распространять при помощи захваченного домена сведения, позорящие потерпевшего или причиняющие ему существенный вред, например, распространять негативные сведения от его лица.

Хороший пример такого поведения все желающие могли наблюдать в 2003 году, когда неустановленные лица зарегистрировали доменное имя gprf.info и разместили под ним сайт, якобы принадлежащий Генеральной прокуратуре РФ (у прокуратуры тогда своего сайта не было). Среди прочей информации, сведений о руководителях и новостей на лжесайте были размещены отчеты об исполнении политических заказов, расценки на «услуги» прокуроров и другие подобные материалы [W07, W08, W09].

Также можно припомнить историю с предвыборными сайтами кандидата в мэры Москвы – `lugkov.ru` (сайт сторонников) и `lujkov.ru` (сайт противников).

По имеющимся у автора сведениям, подобными публичными скандалами закончилось всего несколько случаев. В большинстве случаев публичный человек или организация, шантажируемые возможностью такого лжесайта, предпочитали не доводить дело до его появления и решать вопрос тем или иным способом.

Другое

Платежи через Интернет

Это, конечно же, не вид преступления. Однако некоторые чисто офлайновые преступления превращаются в компьютерные, если для передачи денег используются платежные системы Интернета, либо договоренность о платеже достигается через Интернет. В той части, которая касается такого платежа, расследование должно использовать методы компьютерной криминалистики. С другой стороны, многие компьютерные преступления включают в способ совершения осуществление платежа через подобные системы.

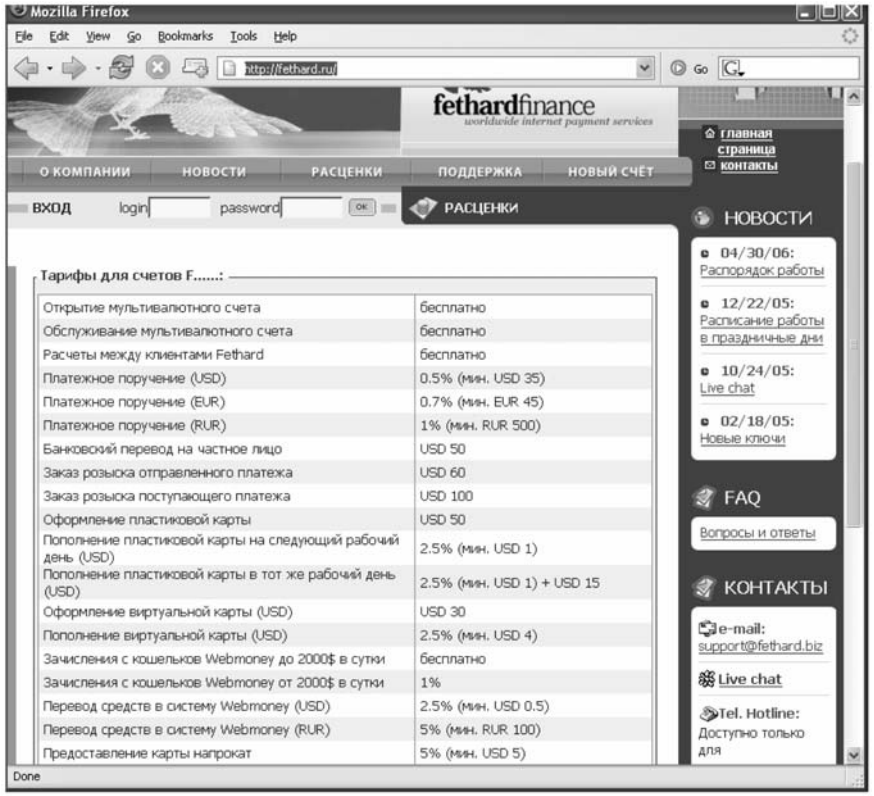
Наряду с банковскими платежными системами и методами платежа, которые подчиняются законодательству той или иной страны и имеют механизмы для расследования проведенных операций, существуют и чисто сетевые платежные системы, которые банками не являются и не столь подвержены контролю со стороны государственных органов. Можно назвать такие системы, как «WebMoney», «PayPal», «E-gold», «Яндекс-Деньги» и другие. Как правило, они связаны между собой различными гейтами и частными посредниками, поэтому можно быстро конвертировать средства из одной системы в другую, затрудняя тем самым отслеживание и блокирование криминальных транзакций. Именно такая квазианонимность и скорость перевода средств привлекают различного рода

злоумышленников к использованию сетевых платежных систем.

Правда, у многих правоохранительных органов есть что называется «оперативные позиции» в таких платежных системах и среди посредников. Иногда их удается задействовать, и тогда транзакции можно не только отследить, но и провести в удобное время удобным для следствия способом, задокументировать или вернуть.

Существуют и вторичные услуги – управление счетами таких платежных систем, ввод и вывод средств из них, в том числе анонимный.

Из-за множественности таких систем, их трансграничности, легкости перевода средств из одной в другую существует реальная возможность остаться анонимным как для плательщика, так и для получателя платежа. Конечно, это не принципиальная анонимность, а трудность отслеживания платежей и переводов.



Открытие мультивалютного счета	бесплатно
Обслуживание мультивалютного счета	бесплатно
Расчеты между клиентами Fethard	бесплатно
Платежное поручение (USD)	0.5% (мин. USD 35)
Платежное поручение (EUR)	0.7% (мин. EUR 45)
Платежное поручение (RUR)	1% (мин. RUR 500)
Банковский перевод на частное лицо	USD 50
Заказ розыска отправленного платежа	USD 60
Заказ розыска поступающего платежа	USD 100
Оформление пластиковой карты	USD 50
Пополнение пластиковой карты на следующий рабочий день (USD)	2.5% (мин. USD 1)
Пополнение пластиковой карты в тот же рабочий день (USD)	2.5% (мин. USD 1) + USD 15
Оформление виртуальной карты (USD)	USD 30
Пополнение виртуальной карты (USD)	2.5% (мин. USD 4)
Зачисления с кошельков Webmoney до 2000$ в сутки	бесплатно
Зачисления с кошельков Webmoney от 2000$ в сутки	1%
Перевод средств в систему Webmoney (USD)	2.5% (мин. USD 0.5)
Перевод средств в систему Webmoney (RUR)	5% (мин. RUR 100)
Предоставление карты напрокат	5% (мин. USD 5)

Перечень услуг одной из посреднических фирм по осуществлению интернет-платежей, вводу и выводу средств. Размер комиссионного вознаграждения явно превышает обычный, но при этом обеспечивается относительная анонимность

Приведем пример из практики. Группа кардеров* для вывода средств, полученных преступным путем, использовали следующий метод. Средства сосредотачивались на нескольких счетах сетевых платежных систем «PayPal» и «E-gold». Как только набиралась заметная сумма, она немедленно перечислялась посреднику – специально созданной ради анонимизации интернет-платежей фирме, которая имела собственные счета в обеих упомянутых платежных системах. По поручению кардеров посредник раз в три месяца открывал новый банковский счет в одном из прибалтийских банков (там не слишком строго проверяют документы у вкладчиков, можно назваться Иваном Петровым или Джоном Смитом, и банкиры поверят на слово). На такой счет сбрасывались криминальные деньги. Банковскую карту от каждого счета вместе с пин-кодом посредник отсылал главарю кардеров по почте на абонентский ящик. Деньги снимались через банкоматы. Все указания как платежным системам, так и посреднику давались через веб-интерфейс или по электронной почте с использованием анонимизирующих прокси-серверов. В результате добытые преступным путем деньги доходили до кардеров с задержкой всего в пару недель и с потерей порядка 40%, зато с высокой степенью анонимности.

Многие сетевые платежные системы выпускают (в сотрудничестве с банками) собственные платежные карты, через которые можно относительно просто вывести деньги, сняв их в любом банкомате. На 2006 год известно о выпуске таких карт для систем:

- Gcard (http://moneymakergroup.ru/-Gcard--t82.html)
- Rupay (http://news.proext.com/money/12310.html)
- Fethard (http://fethard.ru)
- Webmoney (http://cards.webmoney.ru)
- Roboxchange (http://cashcards.ru/WebClient/?Lang=ru&)

Для выпуска карты формально требуется предъявить паспорт или прислать его скан-копию. Но проверка именно формальная, никаких серьезных препятствий для получения карты на чужое имя не существует. Не говоря уже о том, что аккаунты в таких системах свободно продаются и покупаются, можно воспользоваться чужим аккаунтом для заказа карты, которая высылается по почте.

Подобная опция дает злоумышленнику возможность использовать счет «WebMoney» или «E-gold» для получения криминальных платежей, например, доходов от кардерской деятельности, платы от потерпевшего по мошенничеству или вымогательству. Зачисленная на электронный кошелек сумма быстро переводится через два-три промежуточных аккаунта на карточный счет, при этом используется веб-интерфейс управления счетом, который, в принципе, позволяет анонимизировать пользователя. Затем деньги с карты снимаются в банкомате, каковая операция также допускает анонимность.

В порядке противодействия указанным способам, в зависимости от обстоятельств, перед правоохранительными органами могут стоять следующие задачи:

- воспрепятствовать регулярной деятельности злоумышленников, максимально затруднив обналичивание денег с их электронных кошельков;
- воспрепятствовать обналичиванию конкретного платежа на электронный кошелек;
- вернуть конкретный платеж отправителю;
- установить лицо, получающее деньги с конкретного электронного кошелька или получившее конкретный платеж.

Упомянутые выше карты для обналичивания средств с электронных кошельков эмитируются не самими платежными системами (хотя и несут их логотип), а банками. Банки же вполне подконтрольны властям и при наличии судебной санкции не только сообщат всю информацию о карточном счете, но и заблокируют его или вернут платеж.

Когда требуется отследить платеж через банковскую карту, следует обращаться за содействием в соответствующий банк. При наличии судебного решения банк обязан предоставить любую информацию. Чтобы отследить, заблокировать или вернуть платеж внутри сетевой платежной системы, следует обращаться к руководству этой системы. В отличие от банков, они не обременены многочисленными обязанностями перед вкладчиками и ограничениями, поэтому вполне могут себе позволить, например, закрыть счет мошенника и конфисковать все его средства даже без объяснения причины. На сотрудничество с властями электронные платежные системы также идут менее охотно, чем банки. У одних правоохранительных органов могут иметься с ними «хорошие отношения», другие же на свой запрос получат отказ.

Терроризм и кибервойна

Интернет все в большей степени используется для распространения СМИ. Заметна отчетливая тенденция возрастания доли информации, получаемой средним человеком через Сеть. А чем больше информации люди получают через киберпространство, тем более привлекательным оно становится для ведения информационной войны [35, 37, 38, W13].

Информационная война может быть частью войны обыкновенной или вестись отдельно от нее, без развязывания боевых действий. Терроризм же, в отличие от войны, имеет своим обязательным элементом массовую информацию. Современная доктрина определяет терроризм как проведение деструктивных действий с целью запугивания и принуждения, то есть оказания влияния на поведение людей посредством страха [36]. При этом задуманное влияние оказывает не сам теракт (убийство,

взрыв, похищение), а сопровождающее его информационное воздействие через СМИ. То есть без резонанса в СМИ террористический акт перестает быть таковым и превращается в заурядное преступление.

Для ведения информационной войны или информационного обеспечения терактов противник может использовать сетевые СМИ и популярные интернет-ресурсы пассивно – просто сливая в них подготовленную информацию. Но возможно и активное использование Интернета: создание и поддержание собственных интернет-ресурсов, подавление информресурсов противников, провоцирующие действия, навязчивая реклама (спам) и так далее.

Указанные активные действия в Сети могут подпадать под соответствующие статьи УК.

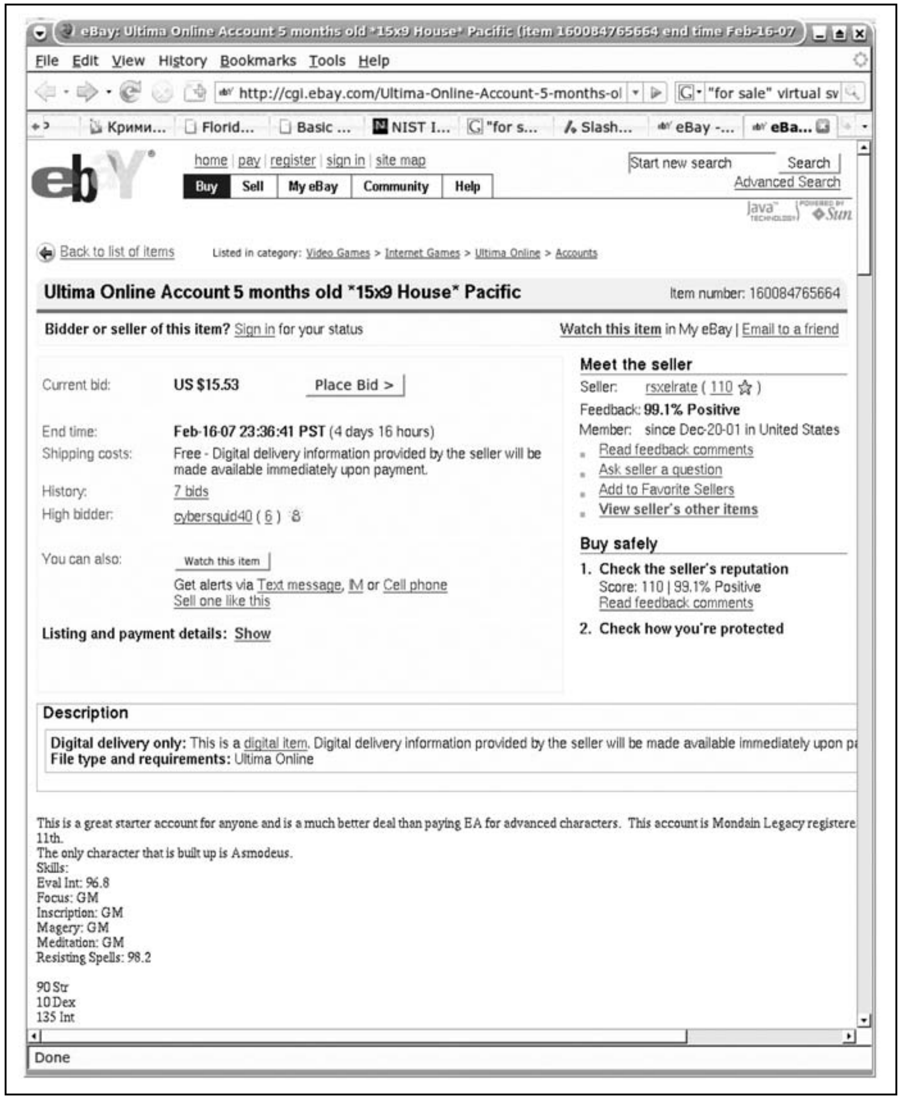
Мошенничество в онлайновых играх

Онлайновые многопользовательские игры, называемые также многопользовательскими мирами или MUD, популярны с начала 1990-х. Однако лишь в начале 2000-х годов они стали коммерциализироваться. Некоторые устроители игр получают основной доход от абонентской платы игроков или продажи лицензий на ПО. Другие проекты делают ставку на торговлю виртуальными предметами, виртуальной недвижимостью и иными предметами и услугами, находящимися целиком внутри виртуального мира. Достаточное число игроков и развитые технические средства делают такие проекты коммерчески успешными.

На аукционах виртуальных предметов совершается сделок на сотни тысяч долларов ежедневно. Продаются виртуальные предметы (оружие, броня, драгоценности, артефакты), персонажи, местная виртуальная валюта, недвижимость виртуального мира (дома, магазины, участки земли под застройку), прочие ценности (разрешения и лицензии от властей виртуального мира, членство в кланах, карты и т.п.) [58].

А там, где появляются ликвидные ценности существенного размера, появляются и мошенники, желающие такие ценности похитить.

В виртуальных мирах возможны различные методы обмана и злоупотреблений. Похищение у персонажей различных ценных виртуальных предметов, а также персонажей целиком. Продвижение персонажа по уровням с использованием недозволенных методов, в том числе уязвимостей в ПО игры (так называемый читинг*). Генерация и дублирование ценных виртуальных предметов. Обман других игроков с целью выманивания у них виртуальных ценностей. Нарушение установленной монополии на различные виды деятельности в виртуальном мире, что ведет к недополучению дохода владельцами игры. Продажа игрокам неразрешенных программных приспособлений для получения игровых преимуществ. И многие другие.



Одно из многочисленных объявлений о продаже ценностей из виртуальных миров за реальные деньги. В данном случае продается персонаж с некоторым количеством виртуального имущества

В некоторых зарубежных странах прошли первые судебные процессы, касающиеся хищения виртуальных предметов и персонажей. В России же интересы игроков не подлежат судебной защите, согласно ст. 1062 ГК. Исключения редки: для некоторых из видов упомянутого типа мошенничества могут использоваться вредоносные программы или неправомерный доступ к игровому серверу. Например, для кражи пароля от игрового персонажа. Но это случай редкий, и относится он к иным видам преступлений, описанным выше.

Автор не исключает, что по мере развития виртуальных миров, нарастания количества их участников, по мере совершенствования возможностей персонажей и, следовательно, возрастания денежных интересов игроков и устроителей такие интересы станут защищаться на государственном уровне, возможно, будут приняты и специальные законы.

Уже сейчас фиксируются сделки с предметами, принадлежащими виртуальному миру, на суммы в десятки тысяч долларов. Уже сейчас есть отдельные лица, зарабатывающие на жизнь участием в таких виртуальных мирах. Прослеживается четкая тенденция к возрастанию размера интересов игроков. Следовательно, скоро потребуется законодательная защита таких интересов.

Использование RBL

RBL (real-time black lists) – это черные списки для защиты от спама, основанные на протоколе DNS. RBL – это как раз тот случай, когда цель не оправдывает средства, когда лекарство становится вреднее болезни.

Исходное предназначение RBL – противодействие рассылке спама. Черный список представляет собой базу данных IP-адресов (реже – доменов), доступную всем пользователям (реже – лишь подписчикам) по протоколу DNS. В запросе указывается IP-адрес. В ответе сообщается, числится ли данный адрес в списке. Большинство мейл-серверов имеют встроенную возможность взаимодействия с любым RBL. При открытии SMTP-сессии принимающий сервер запрашивает RBL, и если IP-адрес передающего мейл-сервера числится, то электронная почта отвергается[1]. Подчеркнем, что входящая почта отвергается без ее принятия, без анализа заголовков или содержания писем, только на основании IP-адреса передающего сервера.

Предполагается, что в RBL должны заноситься источники спама. То есть IP-адреса, с которых часто рассылается спам либо имеется потенциальная возможность этого (например, открытый транслятор электронной почты). Практика показывает, что когда мейл-сервер использует RBL, содержащий источники спама, это приводит к избавлению от значительной части поступающего спама – от 30 до 70%. При этом число ложных срабатываний (то есть случаев, когда отвергается нормальное письмо) хотя и ненулевое, но находится в приемлемых рамках – от 0,1% до 4%, в зависимости от качества используемого черного списка [W22].

[1] Разумеется, эта опция не включена по умолчанию. Фильтрация почты по RBL включается лишь администратором сервера, вполне осознанно.

Далее следует рассказать про RBL, отличающиеся от традиционных. Ввиду наблюдавшегося роста их популярности у некоторых их владельцев появилась идея использовать черные списки в других целях. В некоторые RBL заносятся не источники спама, а IP-адреса провайдеров, политика которых не одобряется держателями черного списка. К неодобряемым чертам провайдеров относятся обычно следующие: (а) предоставление хостинга веб-сайтам, которые рекламируются при помощи спама (так называемые spamvertized-ресурсы); (б) предоставление каких-либо услуг лицу, распространяющему программы или БД, предназначенные для рассылки спама; (в) отказ отключить клиента, обвиненного в вышеуказанных деяниях; (г) отказ отключить субпровайдера, который отказался отключить клиента по одному из вышеуказанных деяний.

Предполагается, что клиенты таких провайдеров, испытывая неудобства в связи с недоставкой своей почты, станут оказывать давление на своих провайдеров, способствуя таким образом изменению их политики в желаемом направлении. Описанные RBL принято называть черными списками второго рода [W23].

Понятно, что занесение в RBL сетей провайдеров является методом реализации убеждений (политических, моральных, нравственных) тех лиц, которые такие черные списки содержат. Не отрицая прав на собственные убеждения и на их пропаганду, тем не менее следует указать, что это не имеет отношения к коммерческой деятельности и, как правило, экономически не обосновано.

От спама использование RBL второго рода также не защищает.

Непосредственные неудобства пользователям создаются не самим RBL, а тем, что некоторые мейл-серверы настроены на его использование. Владелец отвергающего почту мейл-сервера как бы «не отвечает» за факт наличия адреса отправителя в используемом черном списке. Как правило, они не связаны договорными отношениями, а в законодательстве о создании препятствий в передаче электронной почты напрямую не говорится.

Использование чужих RBL для работы мейл-серверов, как правило, не регламентировано внутренними документами компании-провайдера. Часто все подобные настройки делаются рядовыми сотрудниками провайдера без санкции руководства, которое такими «техническими деталями» не интересуется.

В человеческом обществе исторически сложилось так, что в случае вымогательства под угрозой причинения вреда третьему лицу (заложнику) моральная ответственность за последствия ложится не на вымогателя, а на того, кто не исполнил его требования. А действия держателей RBL второго рода как раз и есть аналог захвата заложника: провайдера вынуждают исполнять требования (зачастую незаконные) под угрозой причинения вреда непричастным лицам – его клиентам и клиентам клиентов.

Изобразим схематически отношения между субъектами, вовлеченными в историю с описанным кибервымогательством. Участников можно свести к пяти субъектам.

- отправитель почты;
- администратор передающего мейл-сервера;
- получатель почты;
- администратор принимающего мейл-сервера;
- держатель черного списка.

На самом деле схема несколько сложнее. Над администраторами серверов, как правило, стоят их владельцы (руководители предприятий). В большинстве случаев администраторы делают настройки на использование деструктивных RBL без ведома своего руководства.

Владелец передающего (внесенного в чёрный список) сервера является объектом вымогательства. Его клиент-отправитель письма является непричастным заложником, которому наносится вред. Получателю письма вред также наносится (пунктирная стрелка), но он об этом не знает.

Схема кибервымогательства при помощи RBL немного сложнее, чем классическая схема с заложником. Здесь разнесены субъект, выдвигающий требования, и субъект, непосредственно причиняющий вред непричастному. Держатель черного списка использует администратора принимающего сервера втемную, стараясь не раскрывать ему истинную схему, вводя в заблуждение относительно истинного содержания его RBL.

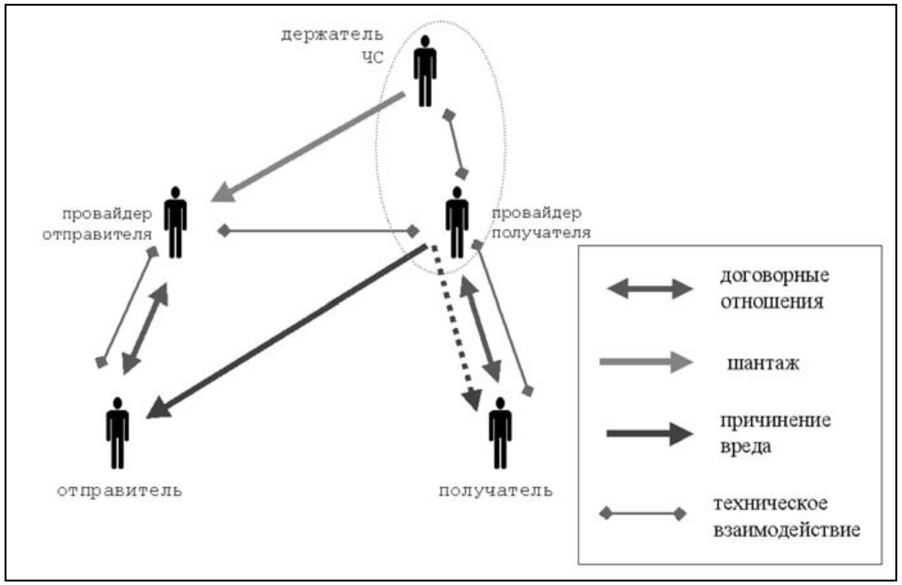


Схема взаимоотношений при шантаже с использованием черного списка (RBL)

Как следует квалифицировать действия держателя RBL второго рода? Сами держатели не отрицают, что их метод подразумевает причинение вреда непричастным. Это официально опубликованная политика таких черных списков, как «Spamhaus», «Sorbs» и «Spews» (ныне не существующего). Держатели RBL выдвигают следующий тезис. Не запрещено публиковать любые списки. Их черный список выражает их собственные «личные» убеждения. Следовательно, его обнародование защищается положениями о свободе слова. Каждый пользователь использует RBL под свою ответственность, на свой собственный риск, о чем имеется предупреждение, опубликованное там же, где и политика RBL.

Действительно, публиковать личные убеждения не может быть запрещено. Однако держатели RBL второго рода делают все, чтобы их деструктивный RBL был похож на обычные RBL первого рода, предназначенные для защиты от спама. Предупреждения относительно политики черного списка и вреда непричастным, мягко говоря, не афишируются. Они изложены хотя и на публичном веб-сайте, но не слишком вразумительно и где-нибудь в конце страницы мелким шрифтом. Держатели RBL второго рода рекламируют свой список как «антиспамовый». Естественно, администратор мейл-сервера, задумав защититься от спама при помощи RBL, просто включает имеющиеся в образцах списки, не изучая подробностей политики каждого из них. Проконтролировать же, какая почта отвергается, не представляется возможным из-за особенностей технологии – напомним, что письмо не принимается, соединение отвергается еще до начала передачи письма. Исследования показывают, что подавляющее большинство пользователей таких RBL были искренне убеждены, что там содержатся лишь источники спама. Подавляющее большинство пользователей отказались от их использования, как только узнали правду.

Таким образом, можно утверждать, что умысел держателя RBL второго рода направлен именно на введение в заблуждение пользователей. Действия держателя RBL могут быть квалифицированы как сознательное причинение вреда непричастным путем обмана или злоупотребления доверием с целью принуждения жертвы к определенным действиям (часто незаконным) в соответствии со своими политическими целями. Вымогательством это считаться не может, поскольку нет требования передачи выкупа. Следовательно, это может быть квалифицировано по ст. 179 УК (принуждение к совершению сделки или к отказу от ее совершения). Аналогичный состав преступления имеется и в законодательстве других стран.

Как следует квалифицировать действия пользователя черного списка? Здесь два варианта.

Если пользователь не знал особенностей RBL второго рода, принимал его за RBL первого рода и использовал именно в качестве такового, то он сам – потерпевший от мошеннических действий, поскольку отвержение валидной электронной почты наносит вред как отправителю, так и получателю, а следовательно, и их провайдерам.

Если же пользователь RBL знал принцип его работы и сознавал, что использование RBL не защищает от спама, а ведет к недоставке валидной почты, то его действия следует квалифицировать как соучастие (ч. 2 ст. 33 УК – соучастие в форме исполнения). Разумеется, сказанное не относится к случаю, когда лицо использует RBL для фильтрации только своей личной почты.

Накрутка

Описанные ниже действия не всегда можно квалифицировать как мошенничество или иное уголовное преступление. Впрочем, даже тогда, когда квалификация возможна, пострадавшие предпочитают не обращаться в правоохранительные органы, а защищаться своими средствами, поскольку это эффективнее.

Накрутка является одним из видов мошенничества с целью хищения средств, ассигнованных на рекламу в сети Интернет, или иного обмана, связанного с рекламой.

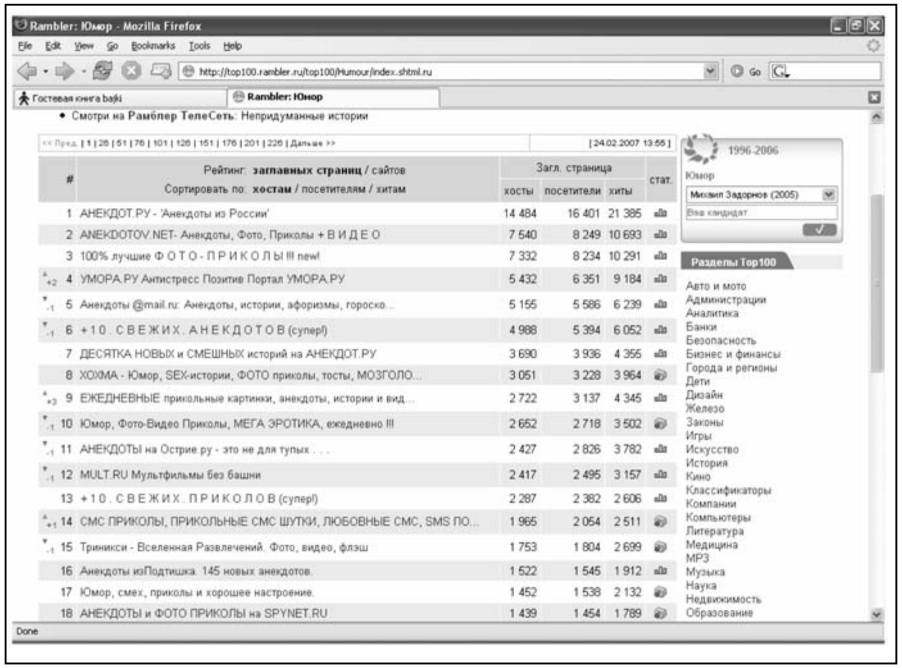
По мере все бóльшей коммерциализации Интернета, по мере увеличения рекламных бюджетов мошенничество с рекламой становится все привлекательнее. Как профессиональные мошенники могут затеять проект с целью обмана рекламодателей или рекламораспространителей, так и обычные владельцы интернет-проектов могут соблазниться легкими, но не вполне честными деньгами.

Доход многих интернет-проектов складывается из поступлений за рекламу. А эти поступления пропорциональны количеству посетителей веб-сайта (или количеству посетителей из целевой аудитории). Таким образом, поднять посещаемость сайта означает пропорционально поднять свои доходы. Между веб-сайтами за посетителей идет нешуточная борьба.

Среди методов увеличения посещаемости есть и не вполне честные методы и даже откровенно мошеннические.

Одним из источников посещаемости веб-сайта (для некоторых – главным источником) являются поисковые системы и интернет-каталоги. Количество пользователей, пришедших по ссылкам из поисковой системы или каталога, сильно зависит от позиции ресурса в результатах поиска или в каталоге. А позиция эта зависит от релевантности запросу (для поисковых систем), от индекса цитируемости или от посещаемости (для каталогов). Поднять свой ресурс в рейтинге можно, сымитировав высокую посещаемость сайта – это и называется накруткой счетчика.

Веб-счетчик – инструмент подсчета посещаемости. Показывается на рейтингуемой веб-странице, но запрашивается с рейтингующего сервера. Измеряет число посетителей и другую статистику для определения рейтинга сайта



Один из рейтингов. Ресурсы упорядочены по посещаемости.
Самые популярные привлекают больше посетителей.
А чем больше посетителей, тем выше позиция в рейтинге.
Один из методов быстро вырваться вперед – накрутить себе посещаемость

Другой способ использования накрутки – непосредственный обман рекламодателя или рекламораспространителя.

При размещении рекламы в Интернете используются три схемы расчета – плата за показ, плата за клик и процент с продаж. В первом случае владельцу рекламной площадки рекламодатель или рекламораспространитель (посредническое рекламное агентство) платит пропорционально числу показов рекламного баннера на веб-странице. Во втором случае плата пропорциональна числу пользователей, перешедших на рекламируемый ресурс по гиперссылке, то есть кликнувших на рекламном баннере*. В третьей схеме рекламораспространитель или владелец рекламной площадки получает от рекламодателя процент с продаж тому клиенту, который пришел по ссылке. Есть и вариант оплаты рекламы по фиксированному тарифу – обусловленная сумма в месяц или в день. Но в этом случае тариф зависит от посещаемости ресурса, на котором реклама размещается.

Первый и второй способы дают возможность для обмана путем манипуляции со статистикой просмотров или статистикой переходов по рекламному баннеру.

Технические методы накрутки статистики весьма разнообразны. Как разнообразны и защитные контрмеры, применяемые рекламодателями и рекламораспространителями, а также поисковыми системами и интернет-каталогами. В ходе накрутки для противодействия этим контрмерам мошенники могут прибегать к использованию зомби-сетей*, вредоносных программ (типа adware*), использовать неправомерный доступ к чужим информационным системам (в том числе к тем, которые ведут статистику) – словом, совершать компьютерные преступления.

Впрочем, большинство случаев накрутки счетчиков, фальсификации статистики или иного недозволенного повышения своих показателей (рейтинга, релевантности, индекса цитируемости) нельзя квалифицировать как уголовные преступления. Это всего лишь нарушение условий договоров, связывающих рекламодателей, рекламораспространителей и владельцев рекламных площадок. С такими нарушениями рекламодатели и посредники должны разбираться самостоятельно, собственными средствами, а возникшие из этого споры относятся к разряду гражданских дел.

Заключение к разделу 1

Теория уголовного права и криминалистика оперируют различными критериями при классификации преступлений. В Уголовном кодексе преступления объединены в статьи по общности объекта преступления, в главы – по общности родового объекта преступления. Криминалистика же характеризует преступления совсем иными параметрами – способ совершения, личность преступника, личность потерпевшего, методы раскрытия и так далее. Оттого и классификация другая. Общую криминалистическую характеристику могут иметь преступления из разных глав УК (например, клевета и возбуждение национальной розни). А преступления, объединенные в одну статью УК, с точки зрения криминалистики, существенно отличны друг от друга (например, нарушение авторских прав в Сети и в офлайне).

Отсюда понятно, что является ошибочным строить криминалистические характеристики преступлений, классифицируя их по критериям уголовного права.

В данном разделе были рассмотрены наиболее распространенные на сегодняшний день виды компьютерных преступлений. Следует помнить, что вследствие развития индустрии ИТ способы совершения киберпреступлений быстро меняются, возникают новые, а старые постепенно сходят на нет.

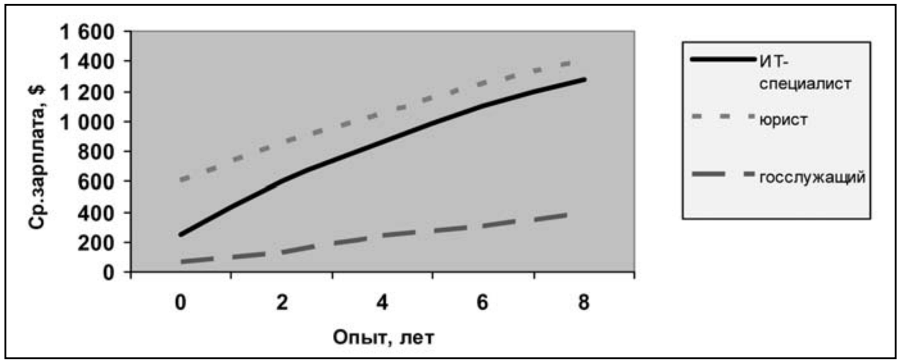
2. Оперативно-розыскные мероприятия

Взаимодействие

При раскрытии компьютерных преступлений на вероятность успеха сильно влияет взаимодействие с двумя видами субъектов: специалистами и операторами связи. Настолько сильной корреляции между содействием с их стороны и успехом раскрытия нет, пожалуй, ни для каких других типов преступлений.

Специальные знания в области ИТ, телекоммуникаций, программирования и защиты информации требуются буквально на каждом этапе – от обнаружения признаков преступления до поддержания обвинения в суде. Источником специальных знаний является специалист. Со стороны следователя или оперуполномоченного было бы слишком самонадеянно рассчитывать на собственные знания в этих областях.

Настоящим ИТ-профессионалом становятся после обучения в вузе и нескольких лет работы по соответствующей специальности. Получить эквивалентные знания, прочитав книги, побеседовав со специалистами и расследовав десяток-другой компьютерных преступлений, никак не возможно. Хотя иллюзия всезнания может возникнуть. Ею часто страдают начинающие. Для таких даже существует особый термин «ламер*», то есть дилетант, «чайник*», который считает себя знающим. Видимо, специфика нашей отрасли такова, что в процессе обучения довольно трудно увидеть свой «горизонт незнания», чтобы адекватно оценить собственный уровень.



Зависимость средней зарплаты от опыта работы (на 2000 год). Для специалистов в области информационных технологий и связи рост быстрее, то есть опыт ценится выше

Как бы сами себя ни оценивали служащие правоохранительных органов, но, как говорится, со стороны виднее. Специалиста с должным уровнем квалификации в области ИТ и телекоммуникаций в штате МВД или ФСБ иметь невозможно. Зато получить помощь стороннего специалиста не слишком сложно.

Было бы ошибкой привлекать специалиста только лишь тогда, когда дело дойдет до экспертизы или до изъятия компьютерной техники. Специальные знания нужны на самой ранней стадии расследования – при первичной проверке материала, а также при проведении оперативно-розыскных мероприятий.

Содействие провайдера* (оператора связи) также обязательный элемент расследования, если только в деле что-то связано с публичной компьютерной сетью.

Роль провайдера в деле получения информации о сетях, клиентах и их активности трудно переоценить. Так сложилось исторически, что Интернет возник как чисто техническое устройство. В те начальные времена его можно было рассматривать как сеть, связывающую компьютеры. Соответственно с этим управлялся Интернет техническими специалистами при помощи доступных и понятных им технических методов. С течением времени, с приходом в Сеть массового пользователя, с развитием сетевых форм общения, с возникновением сетевого бизнеса Интернет превратился из технического устройства в среду, где взаимодействуют не устройства, а люди. На Интернет сейчас завязаны многочисленные финансовые, политические, личные интересы множества людей и организаций. Уже даже говорят о целом виртуальном мире. Но методы управления Интернетом пока остаются старыми. Им управляют в основном технические специалисты, не имеющие гуманитарного образования, зачастую не понимающие, что они взаимодействуют с людьми, а не с техникой. Автор даже предлагает рассматривать диалектическое противоречие – противоречие между новыми общественными отношениями в Сети и старыми методами управления Сетью [98].

Возможно, что в скором времени «сетевая власть» от технарей перейдет в руки профессиональных управленцев. Такие тенденции уже отчетливо заметны на всех уровнях – от домовой сети до международных организаций. Но пока в лице провайдера мы имеем все четыре власти в одном лице. Ныне интернет-провайдер выступает в роли полновластного хозяина своего участка, всемогущего и всеведающего.

Внедрение во всех странах комплексов, аналогичных российскому СОРМу, призвано, в частности, исключить взаимодействие с оператором связи, когда требуется получить информацию о работе пользователя в сети, его трафике и так далее. К сожалению, несмотря на отчеты о внедрении таких комплексов, полностью решить эту задачу не удалось. Ни в России, ни в других странах. Без содействия со стороны оператора связи пока невозможно проводить полноценные ОРМ или следственные действия.

Именно поэтому взаимодействие с работниками операторов связи столь важно на всех этапах – от первичной проверки материала до показаний в суде.

Перехват и исследование трафика

Значение

В перечне видов оперативно-розыскной деятельности присутствует «снятие информации с технических каналов связи». Эта универсальная формулировка включает, в частности, и перехват сетевого трафика*.

В российской судебной практике трафик (результаты его экспертизы) почти не использовался в качестве доказательства. Для ведения ОРД трафик также используется крайне редко. Автор полагает, что его следует использовать шире. В криминальной деятельности перехват и анализ трафика (снифинг*) является основой чуть ли не половины всех методов совершения преступлений. В работе ИТ-специалистов анализ сетевого трафика – один из основных методов диагностики и поиска неисправностей. Возможности этого метода велики. Поэтому и в правоохранительной деятельности он должен использоваться как можно шире.

На основе анализа содержимого, а также статистики сетевого трафика можно определить и доказать совершение пользователем многих действий в сети, а также получить информацию об устройстве программ, информационных систем и сетей.

Сбор и анализ сетевого трафика определенного компьютера может заменить изъятие и экспертизу самого́ этого компьютера, поскольку даст такую же информацию, а именно содержимое электронной почты, свидетельства о просмотре веб-сайтов, о размещении информации в Сети, о несанкционированном доступе к удаленным узлам, об использовании контрафактных программ. И в то же время перехватить трафик бывает проще, чем найти и изъять в исправном состоянии компьютер.

Пример

В качестве примера приведем образец перехваченного веб-трафика, то есть трафика при доступе пользователя к веб-сайту. Перехват осуществлен программой «tcpdump», которая относится к классу сниферов* и входит в состав любой операционной системы (кроме Windows). Параметры команды таковы: «`-n`» означает приводить IP-адреса в цифровой нотации, то есть не переводить их в доменные имена; «`-i fxp0`» указывает интерфейс, с которого снимать трафик; «`-v`» включает режим более подробного вывода сведений о пакетах; «`-xX`» означает приводить также символьное представление всех байтов пакета; «`-s 1024`» указывает,

сколько байтов из каждого пакета показывать; параметр «`tcp and port 80`» определяет фильтр, то есть критерии, по которым пакеты включаются или не включаются в выдачу, в данном случае мы перехватываем пакеты протокола TCP, относящиеся к порту 80, то есть к веб-трафику.

Здесь и далее содержимое трафика приводится в одном из вариантов общепринятого формата «hex dump» [49, W18]. Бинарное содержимое каждого пакета показано в шестнадцатеричной системе счисления по 16 байт в строке. Слева указан порядковый номер первого байта строки, справа – представление тех же байтов в виде ASCII-символов.

```
fnn# tcpdump -n -i fxp0 -v -xX -s 1024 'tcp and port 80'
tcpdump: listening on bge0, link-type EN10MB (Ethernet), capture size 1024
bytes

12:07:16.541938 IP (tos 0x0, ttl  64, id 21663, offset 0, flags [DF],
length: 64, bad cksum 0 (->16e3)!) 10.0.4.31.65406 > 81.16.112.7.80: S [bad
tcp cksum cf68 (->c6d1)!] 11159565:11159565(0) win 65535 <mss
1460,nop,nop,sackOK,nop,wscale 1,nop,nop,timestamp 39474456 0>
        0x0000:  000e a6a4 b3cf 0002 a5e7 4133 0800 4500  ..........A3..E.
        0x0010:  0040 549f 4000 4006 0000 0a00 041f 5110  .@T.@.@.......Q.
        0x0020:  7007 ff7e 0050 00aa 480d 0000 0000 b002  p..~.P..H.......
        0x0030:  ffff cf68 0000 0204 05b4 0101 0402 0103  ...h............
        0x0040:  0301 0101 080a 025a 5518 0000 0000        .......ZU.....

12:07:16.617508 IP (tos 0x0, ttl  58, id 40598, offset 0, flags [DF],
length: 64) 81.16.112.7.80 > 10.0.4.31.65406: S [tcp sum ok]
352447028:352447028(0) ack 11159566 win 65535 <mss 1380,nop,wscale
1,nop,nop,timestamp 913842465 39474456,nop,nop,sackOK>
        0x0000:  0002 a5e7 4133 000e a6a4 b3cf 0800 4500  ....A3........E.
        0x0010:  0040 9e96 4000 3a06 d2eb 5110 7007 0a00  .@..@.:...Q.p...
        0x0020:  041f 0050 ff7e 1501 ea34 00aa 480e b012  ...P.~...4..H...
        0x0030:  ffff 7041 0000 0204 0564 0103 0301 0101  ..pA.....d......
        0x0040:  080a 3678 2121 025a 5518 0101 0402        ..6x!!.ZU.....

12:07:16.617558 IP (tos 0x0, ttl  64, id 21664, offset 0, flags [DF],
length: 52, bad cksum 0 (->16ee)!) 10.0.4.31.65406 > 81.16.112.7.80: . [bad
tcp cksum cf5c (->3075)!] ack 1 win 32832 <nop,nop,timestamp 39474464
913842465>
        0x0000:  000e a6a4 b3cf 0002 a5e7 4133 0800 4500  ..........A3..E.
        0x0010:  0034 54a0 4000 4006 0000 0a00 041f 5110  .4T.@.@.......Q.
        0x0020:  7007 ff7e 0050 00aa 480e 1501 ea35 8010  p..~.P..H....5..
        0x0030:  8040 cf5c 0000 0101 080a 025a 5520 3678  .@.\.......ZU.6x
        0x0040:  2121                                       !!

12:07:16.617940 IP (tos 0x0, ttl  64, id 21665, offset 0, flags [DF],
length: 624, bad cksum 0 (->14b1)!) 10.0.4.31.65406 > 81.16.112.7.80: P
[bad tcp cksum d198 (->3a57)!] 1:573(572) ack 1 win 32832 <nop,nop,time-
stamp 39474464 913842465>
        0x0000:  000e a6a4 b3cf 0002 a5e7 4133 0800 4500  ..........A3..E.
        0x0010:  0270 54a1 4000 4006 0000 0a00 041f 5110  .pT.@.@.......Q.
```



```
        0x0020:  7007 ff7e 0050 00aa 480e 1501 ea35 8018  p..~.P..H....5..
        0x0030:  8040 d198 0000 0101 080a 025a 5520 3678  .@.........ZU.6x
        0x0040:  2121 4745 5420 2f63 6769 2d62 696e 2f61  !!GET./cgi-bin/a
        0x0050:  6c6c 6970 5f76 6965 772e 706c 2048 5454  llip_view.pl.HTT
        0x0060:  502f 312e 310d 0a48 6f73 743a 2061 6c6c  P/1.1..Host:.all
        0x0070:  6970 2e73 7461 7274 7465 6c65 636f 6d2e  ip.starttelecom.
        0x0080:  7275 0d0a 5573 6572 2d41 6765 6e74 3a20  ru..User-Agent:.
        0x0090:  4d6f 7a69 6c6c 612f 352e 3020 2858 3131  Mozilla/5.0.(X11
        0x00a0:  3b20 553b 2046 7265 6542 5344 2069 3338  ;.U;.FreeBSD.i38
        0x00b0:  363b 2065 6e2d 5553 3b20 7276 3a31 2e38  6;.en-US;.rv:1.8
        0x00c0:  2e31 2920 4765 636b 6f2f 3230 3036 3131  .1).Gecko/200611
        0x00d0:  3037 2046 6972 6566 6f78 2f32 2e30 0d0a  07.Firefox/2.0..
        0x00e0:  4163 6365 7074 3a20 7465 7874 2f78 6d6c  Accept:.text/xml
        0x00f0:  2c61 7070 6c69 6361 7469 6f6e 2f78 6d6c  ,application/xml
        0x0100:  2c61 7070 6c69 6361 7469 6f6e 2f78 6874  ,application/xht
        0x0110:  6d6c 2b78 6d6c 2c74 6578 742f 6874 6d6c  ml+xml,text/html
        0x0120:  3b71 3d30 2e39 2c74 6578 742f 706c 6169  ;q=0.9,text/plai
        0x0130:  6e3b 713d 302e 382c 696d 6167 652f 706e  n;q=0.8,image/pn
        0x0140:  672c 2a2f 2a3b 713d 302e 350d 0a41 6363  g,*/*;q=0.5..Acc
        0x0150:  6570 742d 4c61 6e67 7561 6765 3a20 7275  ept-Language:.ru
        0x0160:  2c65 6e2d 7573 3b71 3d30 2e37 2c65 6e3b  ,en-us;q=0.7,en;
        0x0170:  713d 302e 330d 0a41 6363 6570 742d 456e  q=0.3..Accept-En
        0x0180:  636f 6469 6e67 3a20 677a 6970 2c64 6566  coding:.gzip,def
        0x0190:  6c61 7465 0d0a 4163 6365 7074 2d43 6861  late..Accept-Cha
        0x01a0:  7273 6574 3a20 4953 4f2d 3838 3539 2d31  rset:.ISO-8859-1
        0x01b0:  2c75 7466 2d38 3b71 3d30 2e37 2c2a 3b71  ,utf-8;q=0.7,*;q
        0x01c0:  3d30 2e37 0d0a 4b65 6570 2d41 6c69 7665  =0.7..Keep-Alive
        0x01d0:  3a20 3330 300d 0a43 6f6e 6e65 6374 696f  :.300..Connectio
        0x01e0:  6e3a 206b 6565 702d 616c 6976 650d 0a52  n:.keep-alive..R
        0x01f0:  6566 6572 6572 3a20 6874 7470 3a2f 2f61  eferer:.http://a
        0x0200:  6c6c 6970 2e73 7461 7274 7465 6c65 636f  llip.startteleco
        0x0210:  6d2e 7275 2f63 6769 2d62 696e 2f61 6c6c  m.ru/cgi-bin/all
        0x0220:  6970 5f76 6965 772e 706c 3f73 7479 7065  ip_view.pl?stype
        0x0230:  3d69 7026 7265 713d 2a0d 0a41 7574 686f  =ip&req=*..Autho
        0x0240:  7269 7a61 7469 6f6e 3a20 4261 7369 6320  rization:.Basic.
        0x0250:  6458 4e6c 636a 6f33 4e7a 6468 4367 3d3d  dXNlcjo3NzdhCg==
        0x0260:  0d0a 4361 6368 652d 436f 6e74 726f 6c3a  ..Cache-Control:
        0x0270:  206d 6178 2d61 6765 3d30 0d0a 0d0a        .max-age=0....

12:07:16.771948 IP (tos 0x0, ttl  58, id 40614, offset 0, flags [DF],
length: 1420) 81.16.112.7.80 > 10.0.4.31.65406: . 1:1369(1368) ack 573 win
32832 <nop,nop,timestamp 913842586 39474464>
        0x0000:  0002 a5e7 4133 000e a6a4 b3cf 0800 4500  ....A3........E.
        0x0010:  058c 9ea6 4000 3a06 cd8f 5110 7007 0a00  ....@.:...Q.p...
        0x0020:  041f 0050 ff7e 1501 ea35 00aa 4a4a 8010  ...P.~...5..JJ..
        0x0030:  8040 2142 0000 0101 080a 3678 219a 025a  .@!B......6x!..Z
        0x0040:  5520 4854 5450 2f31 2e31 2032 3030 204f  U.HTTP/1.1.200.O
        0x0050:  4b0d 0a44 6174 653a 2057 6564 2c20 3133  K..Date:.Wed,.13
        0x0060:  2044 6563 2032 3030 3620 3039 3a30 353a  .Dec.2006.09:05:
        0x0070:  3432 2047 4d54 0d0a 5365 7276 6572 3a20  42.GMT..Server:.
        0x0080:  4170 6163 6865 2f31 2e33 2e33 3420 2855  Apache/1.3.34.(U
        0x0090:  6e69 7829 206d 6f64 5f70 6572 6c2f 312e  nix).mod_perl/1.
        0x00a0:  3239 206d 6f64 5f73 736c 2f32 2e38 2e32  29.mod_ssl/2.8.2
```

```
0x00b0:  3520 4f70 656e 5353 4c2f 302e 392e 3863  5.OpenSSL/0.9.8c
0x00c0:  2072 7573 2f50 4c33 302e 3232 0d0a 4361  .rus/PL30.22..Ca
0x00d0:  6368 652d 436f 6e74 726f 6c3a 206e 6f2d  che-Control:.no-
0x00e0:  6361 6368 650d 0a45 7870 6972 6573 3a20  cache..Expires:.
0x00f0:  4672 692c 2030 3120 4a61 6e20 3139 3830  Fri,.01.Jan.1980
0x0100:  2031 323a 3030 3a30 3020 474d 540d 0a50  .12:00:00.GMT..P
0x0110:  7261 676d 613a 206e 6f2d 6361 6368 650d  ragma:.no-cache.
0x0120:  0a4b 6565 702d 416c 6976 653a 2074 696d  .Keep-Alive:.tim
0x0130:  656f 7574 3d31 352c 206d 6178 3d31 3030  eout=15,.max=100
0x0140:  0d0a 436f 6e6e 6563 7469 6f6e 3a20 4b65  ..Connection:.Ke
0x0150:  6570 2d41 6c69 7665 0d0a 5472 616e 7366  ep-Alive..Transf
0x0160:  6572 2d45 6e63 6f64 696e 673a 2063 6875  er-Encoding:.chu
0x0170:  6e6b 6564 0d0a 436f 6e74 656e 742d 5479  nked..Content-Ty
0x0180:  7065 3a20 7465 7874 2f68 746d 6c3b 2063  pe:.text/html;.c
0x0190:  6861 7273 6574 3d6b 6f69 382d 720d 0a0d  harset=koi8-r...
0x01a0:  0a35 3261 0d0a 3c48 544d 4c3e 0a3c 4845  .52a..<HTML>.<HE
0x01b0:  4144 3e3c 7469 746c 653e 416c 6c2d 4950  AD><title>All-IP
0x01c0:  3c2f 7469 746c 653e 3c2f 4845 4144 3e0a  </title></HEAD>.
0x01d0:  3c42 4f44 5920 6267 636f 6c6f 723d 2345  <BODY.bgcolor=#E
0x01e0:  3545 4345 3920 7465 7874 3d62 6c61 636b  5ECE9.text=black
0x01f0:  206c 6566 746d 6172 6769 6e3d 3136 2072  .leftmargin=16.r
0x0200:  6967 6874 6d61 7267 696e 3d31 3620 746f  ightmargin=16.to
0x0210:  706d 6172 6769 6e3d 3130 2062 6f74 746f  pmargin=10.botto
0x0220:  6d6d 6172 6769 6e3d 3130 206d 6172 6769  mmargin=10.margi
0x0230:  6e68 6569 6768 743d 3130 206d 6172 6769  nheight=10.margi
0x0240:  6e77 6964 7468 3d31 363e 0a20 0a3c 6365  nwidth=16>...<ce
0x0250:  6e74 6572 3e3c 4831 3e49 5020 7365 6172  nter><H1>IP.sear
0x0260:  6368 3c2f 4831 3e3c 2f63 656e 7465 723e  ch</H1></center>
0x0270:  0a3c 7461 626c 6520 626f 7264 6572 3d30  .<table.border=0
0x0280:  2061 6c69 676e 3d63 656e 7465 7220 6365  .align=center.ce
0x0290:  6c6c 7061 6464 696e 673d 373e 3c74 7220  llpadding=7><tr.
0x02a0:  7661 6c69 676e 3d74 6f70 3e3c 7464 2062  valign=top><td.b
0x02b0:  6763 6f6c 6f72 3d23 3631 4332 3945 3e0a  gcolor=#61C29E>.
0x02c0:  3c70 3e3c 464f 524d 206e 616d 653d 2269  <p><FORM.name="i
0x02d0:  7069 6e66 6f22 2061 6374 696f 6e3d 222f  pinfo».action="/
0x02e0:  6367 692d 6269 6e2f 616c 6c69 705f 7669  cgi-bin/allip_vi
0x02f0:  6577 2e70 6c22 204d 4554 484f 443d 4745  ew.pl».METHOD=GE
0x0300:  543e 0a51 7565 7279 3a20 3c69 6e70 7574  T>.Query:.<input
0x0310:  2074 7970 653d 7465 7874 206e 616d 653d  .type=text.name=
0x0320:  7265 7120 7661 6c75 653d 2727 2073 697a  req.value=''.siz
0x0330:  653d 3332 206d 6178 6c65 6e67 7468 3d38  e=32.maxlength=8
0x0340:  303e 203c 696e 7075 7420 7479 7065 3d73  0>.<input.type=s
0x0350:  7562 6d69 7420 7661 6c75 653d 2720 2053  ubmit.value='..S
0x0360:  6561 7263 6820 2027 3e3c 6272 3e0a 3c74  earch..'><br>.<t
0x0370:  6162 6c65 2062 6f72 6465 723d 303e 3c74  able.border=0><t
0x0380:  7220 7661 6c69 676e 3d74 6f70 3e3c 7464  r.valign=top><td
0x0390:  2061 6c69 676e 3d72 6967 6874 3e54 7970  .align=right>Typ
0x03a0:  6520 6f66 2074 6865 2073 6561 7263 683a  e.of.the.search:
0x03b0:  3c2f 7464 3e0a 3c74 6420 616c 6967 6e3d  </td>.<td.align=
0x03c0:  6c65 6674 3e3c 696e 7075 7420 7479 7065  left><input.type
0x03d0:  3d72 6164 696f 206e 616d 653d 7374 7970  =radio.name=styp
0x03e0:  6520 7661 6c75 653d 6970 2063 6865 636b  e.value=ip.check
0x03f0:  6564 3e20 4950 2061 6464 7265 7373 3c62  ed>.IP.address<b
```


Из анализа этого трафика эксперт может сделать следующие выводы:

- Наблюдаемый компьютер использовал IP-адрес `10.0.0.31`.
- Пользователь использовал браузер «Firefox» версии 2.0 (см. строку «`0x00d0`» четвертого пакета) английской версии, но с поддержкой русского языка (см. строку «`0x0150`» четвертого пакета).
- Пользователь использовал ОС «FreeBSD» для процессора типа Intel (см. строку «`0x00a0`» четвёртого пакета).
- Пользователь в 12 часов 7 минут обращался к веб-сайту «`allip.starttelecom.ru`» и просматривал содержимое веб-страницы «`/cgi-bin/allip_view.pl`».
- На указанную веб-страницу пользователь перешел по ссылке со страницы «`allip.starttelecom.ru/cgi-bin/allip_view.pl?stype=ip&req=*`» (см. поле «`Referer`» в строке «`0x01f0`» четвертого пакета).
- При доступе к указанному веб-сайту использовался логин «user» и пароль «`777a`» (см. четвертый пакет, строка «`0x0250`», параметр «`Authorization: Basic`» и далее логин и пароль в кодировке base64).

На взгляд автора, такая экспертиза перехваченного трафика в ряде случаев может заменить экспертизу компьютера пользователя и сервера, к которому он обращался. А если и не заменить совсем, то дополнить, значительно усилив доказательную базу.

Организация перехвата

Ясно, что трафик, относящийся к определенному узлу, проще всего перехватывать вблизи этого узла. По мере удаления от него возрастает техническая сложность перехвата, но зато снижается организационная сложность. По мере удаления от узла падает надежность и, возможно, полнота перехвата трафика, но зато повышается скрытность. Место перехвата трафика в значительной мере определяется наличием возможностей у органа, ведущего ОРД. Для определения мест и методов возможного перехвата обязательно привлечение технического специалиста.

При этом распространенной ошибкой является привлечение специалиста по аппаратуре телефонной связи. Такой специалист, конечно, доступнее, чем ИТ-специалист того же уровня. «Телефонист» лучше разбирается в оборудовании, технологиях и протоколах связи 1-го и 2-го уровня (физический и канальный). Но работать на более высоких уровнях сетевых протоколов (3-7) он не способен. А как раз на этих уровнях лежит большинство возможностей перехвата трафика.

Различных мест и методов для перехвата сетевого трафика слишком много, чтобы перечислить их здесь. Выделим лишь организационные варианты:

- перехват при помощи имеющейся аппаратуры СОРМ;
- перехват средствами оператора связи;

- перехват собственными средствами.

В подавляющем большинстве случаев в перехватываемом трафике может содержаться тайна связи или тайна частной жизни. Поэтому необходимо получать судебное решение. Без судебной санкции возможен перехват своего собственного трафика потерпевшим либо с его письменного разрешения.

Перехват трафика может быть реализован на разных уровнях.

- На физическом уровне:
  - при помощи электрических и оптических разветвителей;
  - при помощи бесконтактных датчиков;
  - при помощи перехвата радиосигнала (для Wi-Fi и других беспроводных протоколов).
- На канальном уровне:
  - при помощи подключения к концентратору* (хабу);
  - при помощи функции зеркалирования порта на коммутаторе* (свиче);
  - при помощи ARP-атак и проксирования трафика;
  - при помощи установки снифера* на целевом или транзитном узле.
- На сетевом уровне:
  - при помощи изменения маршрутизации и проксирования трафика;
  - при помощи встроенных функций межсетевого экрана или системы обнаружения атак (IDS).
- На прикладном уровне:
  - анализом трафика на прокси-сервере (для HTTP-трафика);
  - анализом трафика на сервере электронной почты (для SMTP-трафика).

Формулируя техническое задание для перехвата трафика, следует непременно прикинуть объем информации. При слишком широких условиях соответствующий трафик может достигнуть астрономических величин. Большой объем не уместится на носителе и поэтому не поддастся последующему анализу.

Например, нас интересуют действия пользователя, работающего за домашним компьютером, который подключен к Интернету через местную домовую сеть. В его трафике мы хотели бы найти доказательства неправомерного доступа к удаленным узлам. Было бы ошибкой ставить задачу так: «перехват исходящего и входящего трафика компьютера с IP-адресом `10.0.0.6`». Помимо неправомерного доступа подозреваемый также занимается и другой деятельностью. На его компьютере стоит клиент файлообменных сетей* со средним суммарным трафиком 6 кбайт/с (500 Мбайт за сутки, 50 входящего и 450 исходящего). Кроме того, в домовой сети расположен файловый сервер с набором музыки и фильмов. Поскольку внутренний трафик для пользователей бесплатен и не ограничен, подозреваемый скачивает 1-2 фильма в день и немного музыки (1 Гбайт за сутки). Внутрисетевой служебный трафик составляет за сутки еще порядка 2 Мбайт. Причем все перечисленное – в автоматическом режиме, независимо от присутствия подозреваемого дома. На этом фоне суточные 10 Мбайт веб-трафика, 0,5 Мбайт электронной почты и 0,2 Мбайт по протоколу ICQ просто теряются. А доказательства неправомерного доступа содержатся лишь в последнем пункте. Перехват всего перечисленного трафика (1,5 Гбайт в сутки) за несколько дней потребует диска очень большой емкости, которого может и не оказаться в распоряжении специалиста. И потом найти в этой куче полезные 0,013% будет нелегко.

Если же мы, чтобы исключить внутрисетевой трафик, велим специалисту перехватывать информацию за пределами домовой сети, на выходе из нее, то допустим иную ошибку. Поскольку домовая сеть подключена к Интернету не напрямую, а через устройство, осуществляющее трансляцию IP-адресов (NAT*), то в этой точке мы не сможем отличить трафик подозреваемого от трафика всех других пользователей той же домовой сети.

В описанной ситуации правильная формулировка задания должна выглядеть примерно так: «перехват исходящего и входящего трафика компьютера с MAC-адресом `00:15:f2:20:96:54`, относящегося к протоколам HTTP, telnet, SMTP, POP, IMAP, ICQ и имеющего в качестве IP-адреса назначения (destination) или происхождения (source) какие-либо внешние IP-адреса, то есть, IP-адреса кроме `10.0.0.0/8`».

Анализ и интерпретация перехваченного трафика должны производиться экспертом в ходе КТЭ. Вместо экспертизы можно оформить это как очередное ОРМ, но тогда доказательством в суде перехваченный трафик не будет.

К перехваченному трафику для его анализа необходимо приложить некоторую информацию о конфигурации и состоянии коммуникационного оборудования, чтобы в ходе КТЭ содержимое трафика можно было интерпретировать уверенно, без предположений. Например, в вышеописанном случае для интерпретации понадобится конфигурация коммутатора домовой сети, MAC-таблица на соответствующем его порту, а также конфигурация устройства, производящего трансляцию адресов (NAT).

Шифрованный трафик

Некоторая часть трафика может оказаться зашифрованной. Это касается таких протоколов, как HTTPS, SSH, SMTP/TLS, IPSec и других. В некоторых случаях весь трафик между определенными узлами или сетями подвергается шифрованию – это называется VPN-туннель. Во всех протоколах, даже простейших, сейчас используются стойкие алгоритмы шифрования, дешифровать которые без знания ключа не стоит даже пытаться.

Столкнувшись с зашифрованным трафиком, можно узнать немногое: установить сам факт сетевой активности, ее приблизительный объем, а также установить IP-адреса взаимодействующих узлов (кроме случая VPN-туннеля).

Для решения указанной задачи следует установить, где именно производится шифрование, и перехватывать трафик в том месте, где он идет открытым.

Например, производя перехват трафика на внешнем интерфейсе «vr0» сервера доступа, мы увидели следующую картину:

```
# tcpdump -n -i vr0 -xX -s 256 -c 4

18:15:04.958167 IP 213.148.4.178.5000 > 80.94.84.25.5000: UDP, length: 212
        0x0000:  0040 f435 d7c3 0040 63da 3cda 0800 4500  .@.5...@c.<...E.
        0x0010:  00f0 7bef 0000 4011 7f50 d594 04b2 505e  ..{...@..P....P^
        0x0020:  5419 1388 1388 00dc 659d 423e 673d 2225  T.......e.B>g="%
        0x0030:  3d3e f779 4fb3 ba35 806f b861 cae4 abbb  =>.yO..5.o.a....
        0x0040:  23ca c65c faf7 8950 2fdb 01e4 9eb7 e105  #..\...P/.......
        0x0050:  4601 58f4 e981 2507 7585 2ab0 0002 0bbb  F.X...%.u.*.....
        0x0060:  5246 54e0 0c8e f849 5772 c879 52e1 8373  RFT....IWr.yR..s
        0x0070:  cb25 9815 0e1e 240a fd7a 5e62 bc7e 75a9  .%....$..z^b.~u.
        0x0080:  d13d d834 ac32 79ff ce43 e744 75a7 1d74  .=.4.2y..C.Du..t
        0x0090:  d958 4f1b 82bf 66e5 25ed 3a7d 20e4 3c80  .XO...f.%.:}..<.
        0x00a0:  a747 0a87 f919 0c8e 4d06 610f 4956 f01d  .G......M.a.IV..
        0x00b0:  333f 4921 630d cde8 cd73 4538 1e41 8187  3?I!c....sE8.A..
        0x00c0:  fae6 658d e7be ebf2 68f0 3bb1 3e0d f5ff  ..e.....h.;.>...
        0x00d0:  908e fb90 6c76 1735 c2d6 5874 96b1 1af5  ....lv.5..Xt....
        0x00e0:  45b7 0562 6446 1848 1218 42ad 1e99 39b9  E..bdF.H..B...9.
        0x00f0:  28aa d7e2 7699 4482 499b 0990 a5ee        (...v.D.I.....

18:15:04.958639 IP 213.148.4.178.5000 > 80.94.84.25.5000: UDP, length: 212
        0x0000:  0040 f435 d7c3 0040 63da 3cda 0800 4500  .@.5...@c.<...E.
        0x0010:  00f0 7bf1 0000 4011 7f4e d594 04b2 505e  ..{...@..N....P^
        0x0020:  5419 1388 1388 00dc d69a 654c 24ab 2841  T.........eL$.(A
        0x0030:  8a74 b88b 110b 7d78 ee9d a54b c274 f704  .t....}x...K.t..
        0x0040:  685a 6100 c3a5 d689 cab9 2e04 bcca d4ea  hZa.............
        0x0050:  ede9 c6a2 a8c3 141a d052 cc56 0b90 2018  .........R.V....
        0x0060:  1325 442c 20fb 0a08 a1cd 7592 5926 573b  .%D,......u.Y&W;
        0x0070:  a4ee 17b3 6b37 7a11 fc03 3847 952a 83da  ....k7z...8G.*..
        0x0080:  a825 eaf9 a4d4 2e91 4b5f f2ca ef96 c18d  .%......K_......
        0x0090:  1801 39f4 20d3 117a b57a a5b1 a23c ddf7  ..9....z.z...<..
        0x00a0:  9247 4cd7 d573 1a06 c42d dab0 e64c 7760  .GL..s...-...Lw`
        0x00b0:  7f3f 3a99 8bb2 2c29 f537 a6ce 86dc eb96  .?:...,).7......
        0x00c0:  7897 87e8 4158 78b2 4cd2 736f 9a27 262c  x...AXx.L.so.'&,
        0x00d0:  6541 785e 69ac 46f1 8a4b 5b0a c409 4923  eAx^i.F..K[...I#
        0x00e0:  023b 69a4 b2f0 f2d8 b579 060d 6027 a115  .;i.....y..`'..
        0x00f0:  a5fe 0f61 860d aa2d 1c6b ceb6 f3cc        ...a...-.k....

18:15:05.259010 IP 80.94.84.25.5000 > 213.148.4.178.5000: UDP, length: 100
        0x0000:  0040 63da 3cda 0040 f435 d7c3 0800 4500  .@c.<..@.5....E.
```



```
        0x0010:  0080 b734 0000 3611 4e7b 505e 5419 d594  ...4..6.N{P^T...
        0x0020:  04b2 1388 1388 006c 21db 38f8 3e20 65eb  .......l!.8.>.e.
        0x0030:  dfbc 20ba 5e0a 137e 9ade 447b 0579 0636  ....^..~..D{.y.6
        0x0040:  37e5 43d5 3991 7424 44ee b635 b222 d454  7.C.9.t$D..5.».T
        0x0050:  acee c0a0 2d3b 078d 5e42 aa83 747e 4cfc  ....-;..^B..t~L.
        0x0060:  c577 76d4 785d d27b 553a 2f2b d7de 0d29  .wv.x].{U:/+...)
        0x0070:  985f 1743 3744 ca4a 470d 4097 ec2a 3d0f  ._.C7D.JG.@..*=.
        0x0080:  8eb4 cba6 1854 d08a 18f2 8292 b45a        .....T.......Z

18:15:05.263016 IP 80.94.84.25.5000 > 213.148.4.178.5000: UDP, length: 148
        0x0000:  0040 63da 3cda 0040 f435 d7c3 0800 4500  .@c.<..@.5....E.
        0x0010:  00b0 b735 0000 3611 4e4a 505e 5419 d594  ...5..6.NJP^T...
        0x0020:  04b2 1388 1388 009c de31 9a0d 4907 1e0d  .........1..I...
        0x0030:  0eb6 1425 6892 7903 b778 f0bc 701a be8b  ...%h.y..x..p...
        0x0040:  8416 9337 7019 144a 5270 b623 0037 49c0  ...7p..JRp.#.7I.
        0x0050:  768b 53d8 471c 589f 80fd b48c 21e3 0cf5  v.S.G.X.....!...
        0x0060:  9d27 95ba fb36 6c89 d0ac 9b02 13a1 a170  .'...6l........p
        0x0070:  aaea 9c20 0a30 e192 2773 842b c6f7 f85f  .....0..'s.+..._
        0x0080:  a765 f720 24fd be29 849d 3b3c 206f 528e  .e..$..)..;<.oR.
        0x0090:  d57f 261c 5d8e fe19 e314 e9fc 30d0 1df4  ..&.].......0...
        0x00a0:  9747 48fa ea99 099b 06af 1f1d b80a ed4d  .GH............M
        0x00b0:  4ed6 6e79 aa1c bc21 4845 bbb8 9999        N.ny...!HE....
```

По контенту пакетов очевидно, что мы имеем дело с шифрованным трафиком. Это подтверждается характерным номером порта (5000), который часто используется для организации VPN-туннелей. Перехватывать такой VPN-трафик бессмысленно. Нужно перехватывать его до входа в туннель или после выхода из него. В данном случае, поскольку туннель терминируется на этом же компьютере, достаточно изменить интерфейс перехвата – вместо физического интерфейса «`vr0`» взять виртуальный интерфейс «`tun0`», соответствующий программному VPN-туннелю. То есть запустить снифер* «`tcpdump`» с параметром «`-i tun0`».

```
# tcpdump -n -i tun0 -xX -s 256 -c 6

18:24:58.503902 IP 80.94.84.26.22 > 83.222.198.130.64106: P
954349589:954349781(192) ack 1245249879 win 33000 <nop,nop,timestamp
1169732958 3836952>
        0x0000:  0200 0000 4510 00f4 7e8a 4000 4006 fc90  ....E...~.@.@...
        0x0010:  505e 541a 53de c682 0016 fa6a 38e2 3815  P^T.S......j8.8.
        0x0020:  4a39 0157 8018 80e8 9b06 0000 0101 080a  J9.W............
        0x0030:  45b8 b55e 003a 8c18 812c b31d 3e7a 12a3  E..^.:...,..>z..
        0x0040:  90d6 db8b c515 f6fb c344 7b0c 4527 6950  .........D{.E'iP
        0x0050:  f7da 74ef 2653 e64e bbd4 35f1 1c7b f23b  ..t.&S.N..5..{.;
        0x0060:  049f d235 2907 65e5 1cce ea52 5480 e4c6  ...5).e....RT...
        0x0070:  6a73 bf84 8d44 b90b 0bd1 3182 2d17 4014  js...D....1.-.@.
        0x0080:  d0ef e13b ecf0 8635 8670 d620 d31c 6249  ...;...5.p....bI
        0x0090:  031a 4e9f b267 0ea7 8325 f85b e9e6 8aab  ..N..g...%.[....
        0x00a0:  f843 1722 b71e bf45 7664 cccb 3de9 3bd7  .C.»...Evd..=.;.
```

```
        0x00b0:  579a 33f2 24d6 6a0f 763b 4033 db8b 23c3  W.3.$.j.v;@3..#.
        0x00c0:  dd57 e1f2 e903 a93a 1cdd 6a0c d27e 4390  .W.....:..j..~C.
        0x00d0:  4523 c955 c5ec e8ee 0899 1d0b 1e91 b52b  E#.U...........+
        0x00e0:  4af6 31a4 28c3 34e5 d890 3966 bdb3 17f8  J.1.(.4...9f....
        0x00f0:  a1f1 ccdb 2504 bf3c                        ....%..<

18:24:58.672890 IP 83.222.198.130.64106 > 80.94.84.26.22: . ack 192 win
32904 <nop,nop,timestamp 3836981 1169732957>
        0x0000:  0200 0000 4500 0034 6936 4000 3606 1cb5  ....E..4i6@.6...
        0x0010:  53de c682 505e 541a fa6a 0016 4a39 0157  S...P^T..j..J9.W
        0x0020:  38e2 38d5 8010 8088 f80d 0000 0101 080a  8.8.............
        0x0030:  003a 8c35 45b8 b55d                        .:.5E..]

18:24:58.763472 IP 80.94.110.110.3727 > 80.94.84.26.445: S
3023694823:3023694823(0) win 16384 <mss 1212,nop,nop,sackOK>
        0x0000:  0200 0000 4500 0030 bd5f 4000 7406 e623  ....E..0._@.t..#
        0x0010:  505e 6e6e 505e 541a 0e8f 01bd b439 ebe7  P^nnP^T......9..
        0x0020:  0000 0000 7002 4000 3065 0000 0204 04bc  ....p.@.0e......
        0x0030:  0101 0402                                   ....

18:24:58.889058 IP 83.222.198.130 > 80.94.84.26: icmp 64: echo request seq
927
        0x0000:  0200 0000 4500 0054 6937 0000 3601 5c99  ....E..Ti7..6.\.
        0x0010:  53de c682 505e 541a 0800 1c73 4e39 039f  S...P^T....sN9..
        0x0020:  45b6 298a 000e 2f63 0809 0a0b 0c0d 0e0f  E.).../c........
        0x0030:  1011 1213 1415 1617 1819 1a1b 1c1d 1e1f  ................
        0x0040:  2021 2223 2425 2627 2829 2a2b 2c2d 2e2f  .!"#$%&'()*+,-./
        0x0050:  3031 3233 3435 3637                        01234567

18:24:58.894094 IP 80.94.84.26.25 > 10.5.0.1.59816: P 1:86(85) ack 1 win
33000 <nop,nop,timestamp 1169744268 483531548>
        0x0000:  0200 0000 4500 0089 7ee2 4000 4006 0d0f  ....E...~.@.@...
        0x0010:  505e 541a 0a05 0001 0019 e9a8 6640 b1dc  P^T.........f@..
        0x0020:  791d 6448 8018 80e8 3420 0000 0101 080a  y.dH....4.......
        0x0030:  45b8 e18c 1cd2 1b1c 3232 3020 686f 6d65  E.......220.home
        0x0040:  2e66 6e6e 2e72 7520 4553 4d54 5020 5365  .fnn.ru.ESMTP.Se
        0x0050:  6e64 6d61 696c 2038 2e31 332e 312f 382e  ndmail.8.13.1/8.
        0x0060:  3133 2e31 3b20 5475 652c 2032 3320 4a61  13.1;.Tue,.23.Ja
        0x0070:  6e20 3230 3037 2031 383a 3236 3a35 3120  n.2007.18:26:51.
        0x0080:  2b30 3330 3020 284d 534b 290d 0a          +0300.(MSK)..

18:24:58.984199 IP 10.5.0.1.59816 > 80.94.84.26.25: P 1:19(18) ack 86 win
33000 <nop,nop,timestamp 483531595 1169744268>
        0x0000:  0200 0000 4500 0046 dac3 4000 4006 b170  ....E..F..@.@..p
        0x0010:  0a05 0001 505e 541a e9a8 0019 791d 6448  ....P^T.....y.dH
        0x0020:  6640 b231 8018 80e8 2595 0000 0101 080a  f@.1....%.......
        0x0030:  1cd2 1b4b 45b8 e18c 4548 4c4f 2061 6968  ...KE...EHLO.aih
        0x0040:  732e 666e 6e2e 7275 0d0a                  s.fnn.ru..
```

И мы увидим тот же трафик, но уже вне VPN-туннеля. Из шести видимых пакетов 3-й относится к протоколу NETBIOS, 4-й – к протоколу ICMP, 5-й и 6-й пакеты – к протоколу SMTP. А контент первых двух пакетов по-прежнему зашифрован: эти пакеты относятся к протоколу SSH со встроенным шифрованием. Получить их в открытом виде перехватом трафика в ином месте нельзя, поскольку шифрование здесь происходит на более высоком уровне (6).

Кстати, этот пример еще раз подтверждает высказанный ранее тезис, что при перехвате сетевого трафика необходимо знать сопутствующую конфигурацию оборудования. В данном примере – конфигурацию интерфейсов сервера доступа. Только благодаря знанию этой конфигурации мы определили, где следует перехватывать трафик, чтобы получить его в нешифрованном состоянии.

Исследование статистики трафика

Статистика прошедшего трафика собирается на многих устройствах. Все без исключения маршрутизаторы, а также многие иные коммуникационные устройства имеют встроенные функции для сбора разнообразной статистики.

Статистика – это, конечно, не перехват трафика, она не дает доступа к его содержимому. Но и из статистики можно немало почерпнуть для расследования и для доказательства компьютерных преступлений.

В простейших случаях на каждом интерфейсе подсчитывается лишь общее количество полученных и отправленных байтов и пакетов. Настройки по умолчанию предполагают более подробную статистику. Полное архивирование всего трафика ведется лишь в редких случаях и не для всех протоколов.

Netflow

Часто статистика ведется по формату «netflow». Он предусматривает запись сведений о каждом «потоке» (flow), то есть серии пакетов, объединенных совокупностью IP-адресов, портов и номером протокола [45, 46]. По такой статистике можно установить:

- факт обращения определенного узла (компьютера, идентифицированного IP-адресом) к другому узлу;
- время обращения с точностью до интервала дискретизации (от 5 минут до 1 часа);
- количество переданного и полученного трафика;
- протокол;
- номера портов с обеих сторон (для TCP и UDP).

Пример

Приведем пример, как при помощи статистики трафика можно получить ценную оперативную информацию.

Потерпевшим было получено сообщение электронной почты, отправленное злоумышленником через анонимайзер «remailer@aarg.net». Анонимайзер – это сервер электронной почты, который специально предназначен для сокрытия отправителя (подробнее об анонимайзерах – ниже, в параграфе «Анонимные ремейлеры»). Служебные заголовки сообщения не содержали никакой полезной информации. Логи анонимайзером не ведутся из принципа.

Для вычисления отправителя можно воспользоваться статистикой трафика.

Для начала сделаем следующие предположения: отправитель находится в России, и он отправил свое сообщение на этот анонимайзер непосредственно, а не через другой анонимайзер. При таких условиях можно попытаться вычислить отправителя.

IP-адрес анонимайзера «remailer@aarg.net» - 206.132.3.41. Письмо к потерпевшему пришло 20 января вечером. Значит, отправлено было, скорее всего, в этот же день, поскольку, хотя анонимайзер предусматривает задержку в доставке сообщений, но вводить слишком большую задержку бессмысленно. Будем искать в статистике российских магистральных операторов связи все обращения на IP-адрес 206.132.3.41, совершенные в течение суток 20.01.07 по протоколу SMTP. Для просмотра статистики используем набор утилит «flow tools».

Итак, для начала, проверим, на какие IP-адреса были обращения за нужную дату по протоколу TCP, на порт 25 (SMTP). Нижеприведенная команда берёт хранящуюся на сервере статистику (`flow-cat`), отфильтровывает из нее протокол TCP (`flow-filter -r6`), отфильтровывает трафик, направленный на порт 25 (`flow-filter -P 25`), и агрегирует данные по IP-адресу назначения (`flow-stat -f8`).

```
fnn@statserver$>flow-cat /data/flows/moscow-bbn/2007/2007-01/2007-01-20/* |
flow-filter -r6 | flow-filter -P 25 | flow-stat -f8 -S3

#  --- ---- ---- Report Information --- --- ---
#
# Fields:    Total
# Symbols:   Disabled
# Sorting:   Descending Field 3
# Name:      Destination IP
#
# Args:      flow-stat -f8 -S3
#
#
# IPaddr          flows                  octets                  packets
#
212.12.0.5        100206                 3074015739              3155006
195.98.64.73      172775                 473707543               947041
213.177.96.24     66199                  553528589               838639
```



```
195.98.64.65      85655                  270256429               748457
82.208.117.5      7989                   837433907               630376
83.221.165.2      615                    872160671               606258
...
85.113.144.109    19                     2036                    38
12.40.224.88      1                      27848                   38
204.136.64.90     1                      28001                   38
213.140.7.76      1                      28447                   38
169.253.4.31      1                      28395                   38
170.148.48.177    1                      28425                   38
193.120.46.86     1                      27824                   38
203.63.58.213     1                      28017                   38
66.151.183.153    1                      28503                   38
12.7.175.31       1                      33541                   38
208.148.192.202   2                      27997                   38
209.47.66.10      1                      28437                   38
85.10.215.4       1                      28365                   38
204.58.248.20     1                      28425                   38
12.4.27.60        1                      28401                   38
12.47.209.186     1                      28413                   38
66.150.143.146    1                      27860                   38
148.235.52.9      1                      27977                   38
128.83.32.61      1                      28431                   38
211.76.152.8      1                      28431                   38
206.132.3.41      2                      27995                   38
203.77.177.12     1                      28485                   38
192.44.63.50      1                      28449                   38
204.64.38.10      1                      27864                   38
202.57.99.9       1                      29005                   38
...
```

В списке DST-адресов (адресов назначения) мы видим интересующий нас адрес 206.132.3.41 (пятая строка снизу), причем на него зафиксировано 2 обращения (flow), всего 38 пакетов, 27995 байт. Такое небольшое количество пакетов за целые сутки неудивительно. Анонимайзерами пользуются нечасто, поскольку это хоть и относительно безопасно, но не слишком удобно.

Выше мы запрашивали статистику за сутки. Поскольку статистика собирается с интервалом в 15 минут, поинтересуемся, в какой именно интервал времени в течение суток были зафиксированы эти обращения. Поищем их в каждом из четвертьчасовых файлов. То есть произведем поиск, аналогичный предыдущему, но не для всей суточной статистики, а для каждого из 15-минутных интервалов (команда «`for f in … do`»).

```
fnn@statserver$>for f in /data/flows/moscow-bbn/2007/2007-01/2007-01-20/*;
do ls ${f}; flow-cat ${f} | flow-filter -r6 | flow-filter -P 25 | flow-stat
-f8 -S3 | grep "206.132.3.41"; done
```

```
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.000000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.001500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.003000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.004500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.010000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.011500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.013000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.014500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.020000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.021500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.023000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.024500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.030000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.031500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.033000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.034500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.040000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.041500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.043000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.044500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.050000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.051500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.053000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.054500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.060000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.061500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.063000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.064500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.070000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.071500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.073000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.074500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.080000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.081500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.083000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.084500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.090000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.091500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.093000+0300
206.132.3.41      1                    27899                   36
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.094500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.100000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.101500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.103000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.104500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.110000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.111500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.113000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.114500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.120000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.121500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.123000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.124500+0300
```



```
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.130000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.131500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.133000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.134500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.140000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.141500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.143000+0300
206.132.3.41      1                    96                      2
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.144500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.150000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.151500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.153000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.154500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.160000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.161500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.163000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.164500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.170000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.171500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.173000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.174500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.180000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.181500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.183000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.184500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.190000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.191500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.193000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.194500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.200000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.201500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.203000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.204500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.210000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.211500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.213000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.214500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.220000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.221500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.223000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.224500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.230000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.231500+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.233000+0300
/data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-v05.2007-01-20.234500+0300
fnn@statserver$>
```

Упоминание искомого IP-адреса нашлось в 2 из 96 файлов. Оказалось, что обращения происходили в интервале 9:30-9:45 и 14:30-14:45, причем во втором случае было передано лишь 2 пакета, а этого недостаточно для полноценной SMTP-сессии. Таким образом, все данные следует искать в файле, содержащем статистику за 9:30-9:45.

```
fnn@statserver$>flow-cat /data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-
v05.2007-01-20.093000+0300 | flow-filter -r6 | flow-filter -P 25 | flow-stat
-f8 -S3 | grep "206.132.3.41"
206.132.3.41      1                    27899                    36
fnn@statserver$>
```

Выберем из полной статистики за указанный интервал те пакеты, которые относятся к интересующему нас анонимайзеру. Для этого вместо упорядочивания данных по IP-адресу назначения, как в предыдущих случаях (`flow-stat -f8`), запросим полную статистику (`flow-print`) и выделим из нее утилитой «grep» те потоки, которые относятся к адресу анонимайзера 206.132.3.41.

```
fnn@statserver$>flow-cat /data/flows/moscow-bbn/2007/2007-01/2007-01-20/ft-
v05.2007-01-20.093000+0300 | flow-filter -r6 | flow-filter -P 25 | flow-
print  | egrep "IP|206.132.3.41"

srcIP           dstIP           prot  srcPort  dstPort  octets   packets
81.16.118.238   206.132.3.41    6     4453     25       27899    36
fnn@statserver$>
```

Мы видим, что у всех относящихся к делу пакетов один и тот же source-адрес – 81.16.118.238. Это, скорее всего, и есть IP-адрес отправителя. Переданный объем информации, 27899 байт, примерно соответствует (с учетом служебных заголовков и шифрования) длине сообщения, полученного потерпевшим, что косвенно подтверждает правильность нашего вывода.

Вот таким образом заурядная статистика провайдера позволила нам раскрыть инкогнито злоумышленника, понадеявшегося на анонимный ремейлер.

Другая задача, выполняемая при помощи статистики трафика, это обнаружение источника DoS-атаки или иной атаки с подделанными адресами источника (source IP). По статистике видно, из какого интерфейса пришел на маршрутизатор такой пакет, то есть каков был предыдущий узел в его пути. Обратившись к статистике этого предыдущего узла, мы можем узнать предпредыдущий узел и так далее. К сожалению, это задача непростая, придется устанавливать контакт с несколькими провайдерами. Если один из них откажется сотрудничать или не сохранит статистику, то цепочка оборвется.

Другие данные о трафике

Кроме полного перехвата сетевого трафика и анализа его статистики имеют право на существование промежуточные варианты ОРМ. Полное содержимое трафика может оказаться чересчур объемным, что затрудняет анализ или делает его невозможным в реальном времени. Статистика, напротив, слишком скупа. Промежуточные варианты – это перехват сведений о сетевых соединениях (сессиях) или перехват трафика на основе сигнатур.

Анализ заголовков пакетов

Сведения о сетевых соединениях или о заголовках пакетов – это то ли урезанный перехват трафика (без сохранения сведений о содержимом пакетов, но лишь об их заголовках), то ли развернутый вариант статистики (когда записывается не агрегированная по времени информация о переданных пакетах).

Например, что можно сказать о компьютере 10.0.4.224, получив следующую информацию о переданных пакетах? Перехват заголовков осуществлялся той же программой «`tcpdump`», что и в примере для главы «Перехват и исследование трафика», но без опций «`-v -xX`». Использованный в этот раз фильтр «`tcp and (net 64.12.0.0/16 or net 205.188.0.0/16)`» выделяет из общего потока те пакеты, которые относятся к сетям `64.12.0.0/16` и `205.188.0.0/16` – это сети, где стоят сервера, обслуживающие ICQ.

```
-bash-2.05b$ sudo tcpdump -i fxp0 -n 'tcp and (net 64.12.0.0/16 or net
205.188.0.0/16)'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on fxp0, link-type EN10MB (Ethernet), capture size 96 bytes

15:53:53.968123 IP 205.188.165.249.80 > 10.0.4.224.1728: . ack 2482877808 win
16384
15:53:54.462314 IP 205.188.165.249.80 > 10.0.4.224.1728: P 0:1122(1122) ack 1 win
16384
15:53:54.514242 IP 10.0.4.224.1728 > 205.188.165.249.80: P 1:617(616) ack 1122
win 64413
15:53:54.521192 IP 10.0.4.224.1729 > 205.188.165.249.80: S
3173139757:3173139757(0) win 65535 <mss 1460,nop,nop,sackOK>
15:53:54.866705 IP 205.188.165.249.80 > 10.0.4.224.1729: S
1561008869:1561008869(0) ack 3173139758 win 16384 <mss 1360>
15:53:54.866882 IP 10.0.4.224.1729 > 205.188.165.249.80: . ack 1 win 65535
15:53:54.867122 IP 10.0.4.224.1729 > 205.188.165.249.80: P 1:261(260) ack 1 win
65535
15:53:55.252895 IP 205.188.165.249.80 > 10.0.4.224.1728: . 1122:2482(1360) ack
617 win 16384
15:53:55.259856 IP 205.188.165.249.80 > 10.0.4.224.1728: . 2482:3842(1360) ack
617 win 16384
15:53:55.260369 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 3842 win 65535
15:53:55.261250 IP 205.188.165.249.80 > 10.0.4.224.1728: . 3842:5202(1360) ack
617 win 16384
15:53:55.462175 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 5202 win 65535
15:53:55.656819 IP 205.188.165.249.80 > 10.0.4.224.1729: . 1:1361(1360) ack 261
win 16384
```

```
15:53:55.763942 IP 10.0.4.224.1729 > 205.188.165.249.80: . ack 1361 win 65535
15:53:55.911588 IP 205.188.165.249.80 > 10.0.4.224.1728: . 5202:6562(1360) ack
617 win 16384
15:53:55.918786 IP 205.188.165.249.80 > 10.0.4.224.1728: . 6562:7922(1360) ack
617 win 16384
15:53:55.919324 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 7922 win 65535
15:53:56.349446 IP 205.188.165.249.80 > 10.0.4.224.1729: P 1361:1770(409) ack 261
win 16384
15:53:56.468076 IP 10.0.4.224.1729 > 205.188.165.249.80: . ack 1770 win 65126
15:53:56.698139 IP 205.188.165.249.80 > 10.0.4.224.1728: . 7922:9282(1360) ack
617 win 16384
15:53:56.699544 IP 205.188.165.249.80 > 10.0.4.224.1728: . 9282:10642(1360) ack
617 win 16384
15:53:56.700065 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 10642 win 65535
15:53:56.705243 IP 205.188.165.249.80 > 10.0.4.224.1728: . 10642:12002(1360) ack
617 win 16384
15:53:56.706685 IP 205.188.165.249.80 > 10.0.4.224.1728: . 12002:13362(1360) ack
617 win 16384
15:53:56.707210 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 13362 win 65535
15:53:57.429094 IP 205.188.165.249.80 > 10.0.4.224.1728: P 13362:13835(473) ack
617 win 16384
15:53:57.574583 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 13835 win 65062
```

Можно сказать, что на компьютере с адресом 10.0.4.224 установлена программа ICQ, которая достаточно активно используется. Причем установлена бесплатная версия этой программы, поскольку наряду с приемом и отправкой сообщений (порт 5190) наблюдается прием рекламных баннеров (порт 80). Содержание передаваемых сообщений из перехваченных заголовков пакетов не видно.

Избирательный перехват

Перехват по сигнатурам используется для защиты информации в таком техническом средстве, как система обнаружения атак (IDS*). Она ищет в передаваемых пакетах заранее предопределенные последовательности байтов, соответствующие попыткам несанкционированного доступа, активности вредоносных программ, иным неразрешенным или подозрительным действиям.

Аналогично можно построить и анализ трафика подозреваемого – предопределить характерные последовательности (сигнатуры), соответствующие подозрительным действиям. И ловить только сессии, в которых встречаются эти сигнатуры. Например, подозреваемый пользуется услугами провайдера коммутируемого доступа и, следовательно, соединяется с Интернетом с использованием динамического* IP-адреса. Наряду с ним IP-адреса из той же сети используют еще несколько сотен пользователей. Требуется проконтролировать переписку подозреваемого по электронной почте. Для этого достаточно записывать все SMTP-сессии, исходящие из сети, где расположен компьютер подозреваемого, в которых встречается последовательность символов «`From: <info@e38.biz>`», чтобы выделить письма, направленные от подозреваемого любым адресатам через любые промежуточные узлы.

Для такого избирательного перехвата можно использовать почти любую IDS. Многие из них поддерживают довольно сложные сигнатуры со многими условиями.

Исследование логов веб-сервера

Значение логов

Автор подметил интересную особенность. Выражения «лог-файлы» или просто «логи*» легко употребляются оперативниками, следователями всеми участниками процесса, однако мало кто из них четко представляет себе, что это такое. Чиновники Минсвязи норовят заставить операторов «хранить логи в течение трех лет», однако затрудняются сказать, какие именно логи и вообще, что это такое. Государственный обвинитель во время процесса лихо ссылается на «логи провайдера», однако когда ему эти логи показывают, в упор их не узнает, удивляясь, что это за невразумительная цифирь.

Технические же специалисты, которые с лог-файлами сталкиваются ежедневно, для которых это неотъемлемая составляющая каждодневной работы, приходят в недоумение от такого вопроса следователя: «Какая информация записывается в лог-файл?» Да любая! Какую вы пожелаете, такая и записывается.

Поэтому автор считает нужным здесь объяснить, что же такое лог-файл или лог.

Лог – это журнал автоматической регистрации событий, которые фиксируются в рамках какой-либо программы. Обычно каждому событию соответствует одна запись в логе. Обычно запись вносится сразу же после события (его начала или окончания). Записи эти складываются в назначенный файл само́й программой либо пересылаются ею другой, специализированной программе, предназначенной для ведения и хранения логов.

Как понятно из определения, в логах могут регистрироваться абсолютно любые события – от прихода единичного ethernet-фрейма до результатов голосования на выборах президента. Форма записи о событии также целиком остается на усмотрение автора программы. Формат лога может быть машинно-ориентированным, а может быть приспособлен для чтения человеком.

Иногда логи ориентированы на цели безопасности и расследования инцидентов. В таких случаях стараются по возможности изолировать логи от системы, события в которой они фиксируют. Если злоумышленник

преодолеет средства защиты и получит доступ в систему, он, возможно, не сможет одновременно получить доступ к логам, чтобы скрыть свои следы.

Почти каждое действие, производимое человеком при взаимодействии с информационной системой, может отражаться в логе прямо или косвенно, иногда даже в нескольких логах одновременно. И логи эти могут быть разбросаны по различным местам, о которых неспециалист даже не догадается.

Чтобы узнать о действиях злоумышленника, получить какие-либо данные о нем при помощи логов, необходимо:

- узнать, какие компьютеры и их программы вовлечены во взаимодействие;
- установить, какие события логируются в каждой из вовлеченных программ;
- получить все указанные логи за соответствующие промежутки времени;
- исследовать записи этих логов, сопоставить их друг с другом.

Вот, например, такое обыденное действие, как просмотр одним пользователем одной веб-страницы. Перечислим вовлеченные в это действие системы, которые в принципе могут вести логи событий:

- браузер пользователя;
- персональный межсетевой экран на компьютере пользователя;
- антивирусная программа на компьютере пользователя;
- операционная система пользователя;
- DNS-сервер (резолвер*), к которому обращался браузер пользователя перед запросом веб-страницы, а также DNS-сервера (держатели зон), к которым рекурсивно обращался этот резолвер;
- все маршрутизаторы по пути от компьютера пользователя до веб-сервера и до DNS-серверов, а также билинговые системы, на которые эти маршрутизаторы пересылают свою статистику;
- средства защиты (межсетевой экран, система обнаружения атак, антивирус), стоящие перед веб-сервером и вовлеченными DNS-серверами;
- веб-сервер;
- CGI-скрипты, запускаемые веб-сервером;
- веб-сервера всех счетчиков и рекламных баннеров, расположенных на просматриваемой пользователем веб-странице (как правило, они поддерживаются независимыми провайдерами);
- веб-сервер, на который пользователь уходит по гиперссылке с просматриваемой страницы;
- прокси-сервер (если используется);
- АТС пользователя (при коммутируемом соединении с Интернетом – по телефонной линии) или иное оборудование последней мили (xDSL, Wi-Fi, GPRS и т.д.);
- оборудование СОРМ со стороны пользователя и со стороны веб-сервера.

Итого может набраться два-три десятка мест, где откладываются взаимно скоррелированные записи, относящиеся к одному-единственному действию пользователя – просмотру веб-страницы.

При более сложных видах взаимодействия появляется еще больше мест, в которых могут остаться следы действий пользователя [72]. Определить все эти места и указать, к кому именно следует обращаться за соответствующими логами, – это задача для ИТ-специалиста. Даже самый продвинутый следователь не в состоянии его заменить. Поэтому привлечение специалиста в таких случаях обязательно.

Содержание

Логи веб-сервера, как понятно из предыдущего, являются далеко не единственным источником информации о действиях пользователя. Автор даже не станет называть этот источник главным. Один из основных – вот так правильно.

Какие же данные можно найти в логах веб-сервера? Набор таких данных различается в зависимости от типа веб-сервера и его настроек. Чаще всего в логах присутствуют следующие данные:

- IP-адрес клиента;
- время запроса, включая часовой пояс;
- поля HTTP-запроса клиента:
  - идентификатор (логин) пользователя, если присутствует аутентификация,
  - метод,
  - URL запрашиваемой веб-страницы и отдельные его элементы (домен, путь, параметры),
  - версия протокола,
  - истинный IP (при доступе через неанонимный прокси-сервер),
  - идентификационная строка браузера клиента (включая язык и ОС),
  - реферер (referrer), то есть адрес веб-страницы, с которой был осуществлен переход на данную страницу,
  - тип контента ответа веб-сервера (MIME type),
  - любые другие поля;
- код ответа веб-сервера [30] (status code);
- размер ответа веб-сервера (без учета HTTP-заголовка);
- ошибки, происшедшие при доступе к веб-страницам;
- ошибки при запуске CGI-программ.

Можно ли доверять логам?

Какие данные в логах веб-сервера возможно фальсифицировать, не имея доступа к самому веб-серверу?

Только поля HTTP-запроса. Этот запрос полностью формируется на стороне клиента, поэтому при желании злоумышленник может подставить в него любые поля с любыми значениями.

Зафиксированному в логе IP-адресу можно доверять. Конечно, при этом следует помнить, что это может оказаться IP прокси-сервера или сокс-сервера или иного посредника.

Прочие поля – это внутренние данные веб-сервера (код ответа, размер страницы и т.п.), которым также можно доверять.

Для проверки достоверности данных логов веб-сервера применяется сопоставление записей между собой, а также с иными логами.

Приведем пример из практики, иллюстрирующий полезность сопоставления различных логов. Сотрудник службы информационной безопасности интернет-казино, анализируя логи веб-сервера, заметил, что браузер одного из игроков, согласно полям его HTTP-запросов, поддерживает русский язык. При этом IP-адрес числился за Кореей. Указания же на корейский язык не было. Это возбудило подозрения. Сотрудник проверил, с каких еще адресов обращался пользователь под этим аккаунтом. Оказалось, что с единственного IP. Тогда он проверил, какие еще пользователи обращались с этого же IP. Оказалось, что больше никто этот корейский IP-адрес не использовал. Но сотрудник службы безопасности не успокоился и проверил, какие еще были обращения от браузера с таким же набором настроек (язык, версия браузера, версия ОС, разрешение экрана, принимаемые типы данных). Оказалось, что с такого же браузера было зарегистрировано больше 10 аккаунтов. Все эти пользователи приходили с IP-адресов разных стран, причем страна соответствовала имени пользователя, то есть, например, Джон Смит с IP-адресом США, Ву Пак с IP-адресом Кореи, Ганс Мюллер с IP-адресом Германии и так далее. Но идентичный набор настроек браузера всех этих пользователей (включая поддержку русского языка) вызывал большие подозрения. Когда же сотрудник сопоставил периоды активности всех подозрительных пользователей, он увидел, что они не пересекаются и более того – примыкают один к другому. Он понял, что имеет дело с кардером*, который регистрирует аккаунты по краденым карточкам, пользуясь сокс-серверами в разных странах. Дальнейшая проверка это подтвердила.

Исследование системных логов

Логирование событий в операционной системе является одной из трех составляющих безопасности. Имеется в виду модель «AAA» – authentication, authorization, accounting – аутентификация, авторизация, аудит. Запись всех событий, связанных прямо или косвенно с безопасностью системы, и составляет сущность аудита. Логирование само по себе не препятствует злоумышленнику получить несанкционированный доступ к информационной системе. Однако оно повышает вероятность его выявления, а также последующего нахождения и изобличения злоумышленника. Также логирование способствует выявлению уязвимостей защищаемой системы.

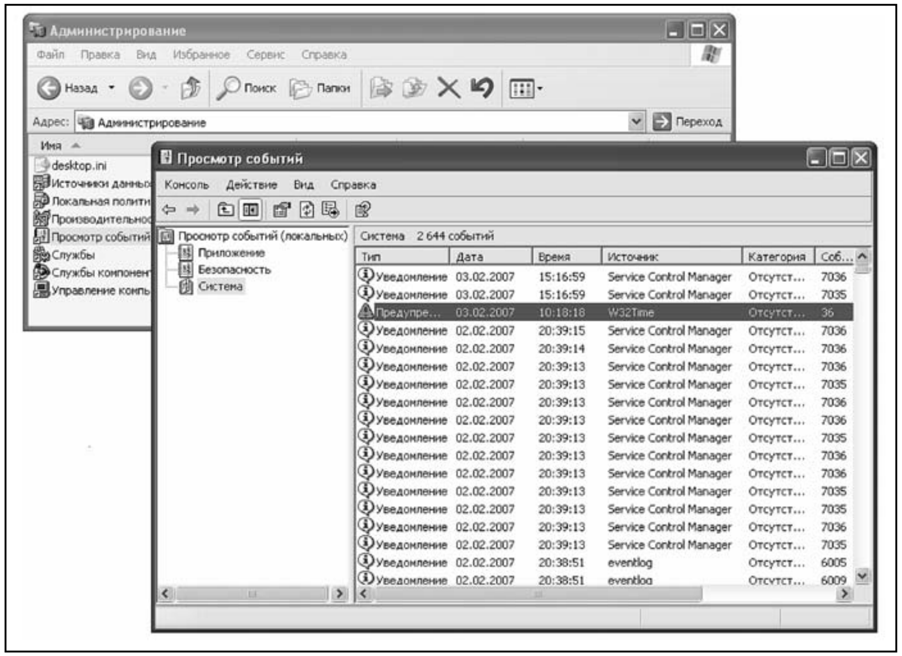
Чем более полон аудит, тем проще расследовать компьютерное преступление. Пользуясь записанными данными, специалист или эксперт может извлечь много полезной для дела информации.

Рассмотрим устройство системного аудита событий для различных классов операционных систем.

Системные логи Windows

В операционных системах линейки «Windows-NT» – «Windows-2000» – «Windows-XP» предусмотрено три лога – прикладных программ (application log), системы (system log) и безопасности (security log).

В application log пишутся сообщения и события, генерируемые прикладными программами, а также некоторыми сервисами (службами). В system log помещаются события ядра ОС и важнейших сервисов. В security log



Программа «Event Viewer» для просмотра логов в Windows

записываются также события, генерируемые системными сервисами, относящиеся к отслеживаемой активности пользователей, их аутентификации и авторизации. К этим трем могут добавляться иные логи, если на компьютере работают дополнительные программы, такие как DNS-сервер.

По умолчанию логируются очень немногие события, а в security log – вообще никаких. Чтобы в логах осаждалась более полная информация, администратор должен явно включить аудит и настроить политики аудита.

Все логи Windows просматриваются специальной программой «Event Viewer», которую можно найти в меню «Administrative Tools» или «Management Console».

В зависимости от того, что именно мы ищем, следы «взлома» исследуемого компьютера или следы противоправной деятельности пользователя, может оказаться полезной разная информация из разных логов.

Системные логи UNIX и Linux

Несмотря на разнообразие UNIX-подобных операционных систем, у всех у них имеется схожая система сбора и хранения системных логов. Логирование событий в операционной системе «MacOS-X» устроено точно таким же образом.

Специальный демон (процесс), называемый `syslogd`, принимает сообщения о событиях от различных программ и процессов и раскладывает их по соответствующим файлам. Сообщения из одного источника можно направить в разные файлы, сообщения от разных источников можно направить в один и тот же файл – система настраивается довольно гибко. Сообщения о событиях можно принимать как локально, так и через сеть; оба способа используют один и тот же протокол [55].

Каждое сообщение при его генерации снабжается двумя идентифицирующими признаками – приоритет (priority) и ресурс (facility). Их сочетание служит для последующей сортировки полученных сообщений по файлам.

Принятые `syslogd` сообщения снабжаются временно́й меткой и записываются в обычный текстовый файл по принципу одно сообщение – одна строка. Просмотреть эти сообщения можно в любом текстовом редакторе или иной программой, умеющей работать с текстовыми файлами.

Системные логи IOS

Значительная часть (если не большинство) коммутаторов и маршрутизаторов сети Интернет работают под управлением операционной системы IOS. Другие ОС для коммуникационного оборудования схожи с IOS своими чертами, в частности, ведут логи аналогичным образом. К таким типичным устройствам относится коммуникационное оборудование, выпущенное под марками «Cisco», «Juniper», «Huawei» и некоторыми другими. Оно составляет подавляющее большинство.

В системе IOS логируются следующие события:

- изменение статуса интерфейса или порта;
- авторизация администратора или устройства;
- изменение и сохранение конфигурации устройства;
- прием транзитного пакета, если такой пакет подпадает под правило (ACL entry), отмеченное флагом логирования;
- некоторые другие.

Сообщения о событиях обычно отсылаются на внешний логирующий сервер по протоколу syslog [55] или SNMP. Также несколько последних сообщений хранятся в буфере, в оперативной памяти и могут быть просмотрены соответствующей командой (show logging).

Когда требуется ознакомиться с логами коммуникационного оборудования, следует проделать такие действия:

- получить доступ к текущей конфигурации устройства (конфигурационному файлу), чтобы определить, куда именно отсылаются логи с данного устройства (команда show running-config); сохранить и задокументировать вышеуказанную конфигурацию (или только ее часть, касающуюся логов);
- (опционально) просмотреть содержимое буфера устройства с последними сообщениями;
- определить местоположение логирующего сервера, то есть сервера, принимающего и сохраняющего логи;
- получить доступ к логирующему серверу и ознакомиться с конфигурацией его syslog-демона, чтобы определить, в какой файл складываются логи, принятые от интересующего нас устройства; сохранить и задокументировать вышеуказанную конфигурацию syslog-демона;
- осмотреть или изъять файл (файлы), в котором сохраняются логи с нужного устройства.

Некоторые коммуникационные устройства, относящиеся к меньшинству, не используют ОС IOS или схожую. В таких нетипичных устройствах логирование может быть устроено иначе. В частности, логи могут храниться локально или передаваться на логирующий сервер по нестандартному протоколу.

Исследование логов мейл-сервера и заголовков электронной почты

Как устроено

Сообщение электронной почты обычно создается на компьютере отправителя в специализированной программе, называемой клиентом электронной почты (MUA – mail user agent). Затем оно отправляется на сервер электронной почты (MTA – mail transfer agent) отправителя. Отту-

да – на сервер электронной почты получателя, возможно, через промежуточный сервер электронной почты (релей). На сервере получателя сообщение помещается в почтовый ящик соответствующего пользователя. Из этого ящика при посредстве сервера доставки (MDA) пользователь забирает сообщение при помощи своей программы-клиента электронной почты (MUA).

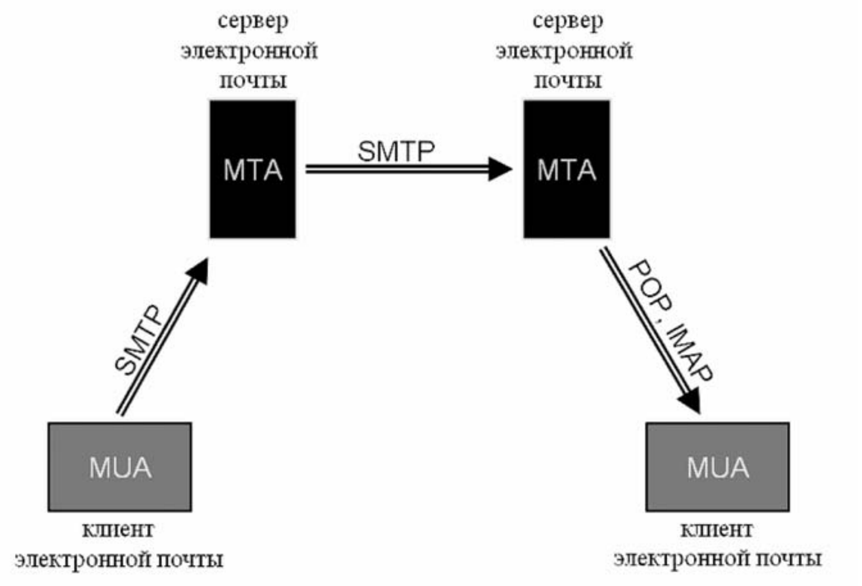


Схема организации передачи электронной почты

Сообщение обычно сохраняется в клиенте (MUA) отправителя и получателя. При прохождении через сервер (MTA) копия сообщения не сохраняется, однако делается запись в логе о его получении и отправке. Также при этом в сообщение вставляется служебный заголовок «`Received`» – так называемый маршрутный заголовок.

Вместо программы-клиента электронной почты (MUA) отправитель и получатель могут использовать веб-интерфейс сервера электронной почты. Он выполняет те же функции, что и клиент, но работает обычно «вблизи» соответствующего MTA (на том же компьютере или на соседнем). Связь отправителя или получателя с веб-интерфейсом происходит при посредстве браузера.

Следы

Таким образом, при прохождении сообщения от отправителя к получателю остаются следующие основные следы:

- копия сообщения на компьютере отправителя;
- запись в логе каждого MTA*, через который сообщение прошло;
- копия сообщения на компьютере получателя с добавленными по пути заголовками.

Кроме того, можно обнаружить дополнительные следы, свидетельствующие о прохождении сообщения:

- иные следы на компьютере отправителя (в логах сетевых соединений, антивируса, персонального межсетевого экрана и т.д.);
- следы в логах провайдеров (например, статистика трафика), через которых осуществлялось соединение между MUA отправителя и MTA отправителя;
- записи в логах антивирусных и антиспамовых программ на всех MTA, через которые прошло сообщение;
- следы, образовавшиеся вследствие обращения всех MTA, через которые прошло сообщение, к соответствующим DNS-серверам как во время приема, так и передачи сообщения;
- следы в логах провайдеров, через которых осуществлялось соединение между MUA получателя и MDA/MTA получателя;
- иные следы на компьютере получателя (в логах сетевых соединений, антивируса, персонального межсетевого экрана и т.д.).

В случаях использования вместо MUA веб-интерфейса к перечисленным следам добавляются следы, характерные для просмотра веб-страниц (см. главу «Исследование логов веб-сервера»). Более подробно об оставляемых следах можно узнать в специализированной литературе [5, 31, 59].

Примеры

Все примеры в этой главе содержат подлинные данные без изъятий, исправлений и дополнений от автора.

Сообщение электронной почты, отложившееся в архиве исходящих сообщений отправителя:

```
From: Nikolay Nikolaevich Fedotov <fnn@starttelecom.ru>
Organization: Start-Telecom
To: fnn@fnn.ru
Subject: Path test
Date: Fri, 15 Dec 2006 16:00:05 +0300
User-Agent: KMail/1.9.4
X-KMail-Transport: Corporate
MIME-Version: 1.0
Content-Type: text/plain;
  charset="koi8-r"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
Message-Id: <200612151600.05273.fnn@starttelecom.ru>
Status: RO
```

```
X-Status: RSC
X-KMail-EncryptionState: N
X-KMail-SignatureState: N
X-KMail-MDN-Sent:

path test
--
Nikolay N Fedotov
Information Security Officer
Start Telecom Inc. (Russia)
```

Два фрагмента лога MTA отправителя (прием и передача). Взяты с сервера mail.starttelecom.ru, он же mail1.wimax.ru:

```
16:00:35.57 4 SMTPI-21885([83.222.198.130]) got connection on
[81.16.112.3:25](wimax.ru) from [83.222.198.130:51746]
16:00:35.71 4 SMTPI-21885([83.222.198.130]) rsp: 220 mail1.wimax.ru
ESMTP CommuniGate Pro 5.0.9
16:00:35.80 4 SMTPI-21885([83.222.198.130]) cmd: EHLO fnn.starttele-
com.ru
16:00:35.80 3 DNR-15700(fnn.starttelecom.ru) A:host name is unknown
16:00:35.80 3 SMTPI-21885(fnn.starttelecom.ru) failed to resolve
HELO parameter: host name is unknown. Real address is
[83.222.198.130]
16:00:35.80 4 SMTPI-21885([83.222.198.130]) rsp: 250-mail1.wimax.ru
host name is unknown fnn.starttelecom.ru\r\n250-DSN\r\n250-SIZE
104857600\r\n250-STARTTLS\r\n250-AUTH LOGIN PLAIN CRAM-MD5 DIGEST-
MD5 GSSAPI MSN NTLM\r\n250-ETRN\r\n250-TURN\r\n250-ATRN\r\n250-NO-
SOLICITING\r\n250-8BITMIME\r\n250-HE
16:00:35.84 4 SMTPI-21885([83.222.198.130]) cmd: STARTTLS
16:00:35.84 4 SMTPI-21885([83.222.198.130]) rsp: 220 please start a
TLS connection
16:00:35.90 4 SMTPI-21885([83.222.198.130]) TLSv1 client hello:
method=RC4_SHA, residual=0, session=34247 < 00 00 85 C7 45 82 9C 73
42 FF 69 04 BF 61 AC 45 0F 1E 45 40 1F B0 BE 2C 72 92 44 C2 F2 55
4D 38>
16:00:35.90 4 SMTPI-21885([83.222.198.130]) TLS handshake: sending
'server_hello'
16:00:35.90 4 SMTPI-21885([83.222.198.130]) TLS handshake: sending
the certificate
16:00:35.90 4 SMTPI-21885([83.222.198.130]) TLS handshake: sending
'hello_done'
16:00:36.07 4 SMTPI-21885([83.222.198.130]) TLS client key exchange
processed
16:00:36.07 4 SMTPI-21885([83.222.198.130]) security initiated
16:00:36.07 4 SMTPI-21885([83.222.198.130]) TLS 'change cipher'
processed
16:00:36.07 4 SMTPI-21885([83.222.198.130]) TLS 'change cipher'
sending
16:00:36.07 4 SMTPI-21885([83.222.198.130]) TLS 'finish handshake'
processed
16:00:36.07 4 SMTPI-21885([83.222.198.130]) TLS handshake: sending
```



```
'finished'
16:00:36.07 4 SMTPI-21885([83.222.198.130]) TLS(RC4_SHA) connection
accepted for 'wimax.ru', session 34247
16:00:36.28 4 SMTPI-21885([83.222.198.130]) cmd: EHLO fnn.starttele-
com.ru
16:00:36.29 3 DNR-15701(fnn.starttelecom.ru) A:host name is unknown
16:00:36.29 3 SMTPI-21885(fnn.starttelecom.ru) failed to resolve
HELO parameter: host name is unknown. Real address is
[83.222.198.130]
16:00:36.29 4 SMTPI-21885([83.222.198.130]) rsp: 250-mail1.wimax.ru
host name is unknown fnn.starttelecom.ru\r\n250-DSN\r\n250-SIZE
104857600\r\n250-AUTH LOGIN PLAIN CRAM-MD5 DIGEST-MD5 GSSAPI MSN
NTLM\r\n250-ETRN\r\n250-TURN\r\n250-ATRN\r\n250-NO-SOLICITING\r\n250-
8BITMIME\r\n250-HELP\r\n250-PIPELI
16:00:36.33 4 SMTPI-21885([83.222.198.130]) cmd: AUTH PLAIN
bi5mZWRvdG92QHN0YXJ0dGVsZWNvbS5ydQBuLmZlZG90b3ZAc3RhcnR0ZWxlY29tLnJ1A
DIzc2Q3c2Rr
16:00:36.46 2 SMTPI-21885([83.222.198.130]) 'n.fedotov@starttele-
com.ru' connected from [83.222.198.130:51746]
16:00:36.46 2 SMTPI-21885([83.222.198.130]) 'n.fedotov@starttele-
com.ru' disconnected ([83.222.198.130:51746])
16:00:37.17 4 SMTPI-21885([83.222.198.130]) rsp: 235
n.fedotov@starttelecom.ru relaying authenticated
16:00:37.22 4 SMTPI-21885([83.222.198.130]) cmd: MAIL
FROM:<fnn@starttelecom.ru> BODY=8BITMIME SIZE=468
16:00:37.22 4 SMTPI-21885([83.222.198.130]) rsp: 250 fnn@starttele-
com.ru sender accepted
16:00:37.22 4 SMTPI-21885([83.222.198.130]) cmd: RCPT
TO:<fnn@fnn.ru>
16:00:37.22 4 SMTPI-21885([83.222.198.130]) rsp: 250 fnn@fnn.ru will
relay mail for an authenticated user
16:00:37.22 4 SMTPI-21885([83.222.198.130]) cmd: DATA
16:00:37.22 4 SMTPI-21885([83.222.198.130]) rsp: 354 Enter mail, end
with "." on a line by itself
16:00:37.30 4 QUEUE([952839]) closed, nOpen=1
...
16:00:39.69 4 SMTP-77633(fnn.ru) connected to mail.fnn.ru
[80.94.84.25:25], ESMTP
16:00:39.69 4 SMTP-77633(fnn.ru) cmd: EHLO mail1.wimax.ru
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-aihs.fnn.ru Hello
mail1.wimax.ru [81.16.112.3], pleased to meet you
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-ENHANCEDSTATUSCODES
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-PIPELINING
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-8BITMIME
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-SIZE
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-DSN
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-ETRN
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250-DELIVERBY
16:00:39.74 4 SMTP-77633(fnn.ru) rsp: 250 HELP
16:00:39.74 4 SMTP-77633(fnn.ru) Connected. DSN SIZE
16:00:39.74 4 SMTP-77633(fnn.ru) [952840] sending
16:00:39.74 4 SMTP-77633(fnn.ru) cmd: MAIL
FROM:<fnn@starttelecom.ru> SIZE=687
```

```
16:00:40.00 4 SMTP-77633(fnn.ru) rsp: 250 2.1.0
<fnn@starttelecom.ru>... Sender ok
16:00:40.00 4 SMTP-77633(fnn.ru) cmd: RCPT TO:<fnn@fnn.ru>
NOTIFY=FAILURE,DELAY
16:00:40.06 4 SMTP-77633(fnn.ru) rsp: 250 2.1.5 <fnn@fnn.ru>...
Recipient ok
16:00:40.06 4 SMTP-77633(fnn.ru) cmd: DATA
16:00:40.11 4 SMTP-77633(fnn.ru) rsp: 354 Enter mail, end with "."
on a line by itself
16:00:40.11 4 QUEUE([952840]) opened, nOpen=3
16:00:40.11 4 QUEUE([952840]) closed, nOpen=2
16:00:40.17 4 SMTP-77633(fnn.ru) rsp: 250 2.0.0 kBFD0bU6010332
Message accepted for delivery
16:00:40.17 2 SMTP-77633(fnn.ru) [952840] sent to [80.94.84.25:25],
got:250 2.0.0 kBFD0bU6010332 Message accepted for delivery
16:00:40.17 4 SMTP(fnn.ru) [952840] batch relayed
16:00:40.17 2 DEQUEUER [952840] SMTP(fnn.ru)fnn@fnn.ru relayed:
relayed via mail.fnn.ru
16:00:40.17 4 QUEUE([952840]) dequeued, nTotal=2
16:00:40.17 4 SMTP-77633(fnn.ru) cmd: QUIT
16:00:40.17 2 QUEUE([952840]) deleted
16:00:40.23 4 SMTP-77633(fnn.ru) rsp: 221 2.0.0 aihs.fnn.ru closing
connection
16:00:40.23 4 SMTP-77633(fnn.ru) closing connection
16:00:40.23 4 SMTP-77633(fnn.ru) releasing stream
```

Обратите внимание на идентификатор соединения «kBFD0bU6010332». Он зафиксирован как в логе этого сервера, так и в логе следующего. Он же будет записан в маршрутном заголовке письма.

Фрагмент лога MTA получателя. Взят с сервера mail.fnn.ru:

```
Dec 15 14:00:38 aihs sm-mta[10332]: kBFD0bU6010332: from=<fnn@start-
telecom.ru>, size=661, class=0, nrcpts=1,
msgid=<200612151600.05273.fnn@starttelecom.ru>, proto=ESMTP,
daemon=IPv4, relay=mail1.wimax.ru [81.16.112.3]

Dec 15 14:00:39 aihs sm-mta[10333]: kBFD0bU6010332: to=fnn@home.fnn,
delay=00:00:01, xdelay=00:00:01, mailer=esmtp, pri=30881,
relay=home.fnn. [80.94.84.26], dsn=2.0.0, stat=Sent (kBFD0g7M018585
Message accepted for delivery)
```

Фрагмент лога второго MTA получателя, на который предыдущий сервер (mail.fnn.ru) пересылает (forward) всю полученную почту. Взят с сервера home.fnn.ru:

```
Dec 15 16:00:43 home sm-mta[18585]: kBFD0g7M018585: from=<fnn@start-
telecom.ru>, size=877, class=0, nrcpts=1,
msgid=<200612151600.05273.fnn@starttelecom.ru>, proto=ESMTP,
daemon=IPv4, relay=aihs-tun [10.5.0.1]
```



```
Dec 15 16:00:43 home sm-mta[18586]: kBFD0g7M018585:
to=<fnn@home.fnn>, delay=00:00:01, xdelay=00:00:00, mailer=local,
pri=31086, relay=local, dsn=2.0.0, stat=Sent
```

Сообщение в почтовом ящике получателя (хранится там временно, до того как получатель заберет свою почту по протоколу POP):

```
From fnn@starttelecom.ru Fri Dec 15 16:00:43 2006
Return-Path: <fnn@starttelecom.ru>
Received: from aihs.fnn.ru (aihs-tun [10.5.0.1])
        by home.fnn.ru (8.13.1/8.13.1) with ESMTP id kBFD0g7M018585
        for <fnn@home.fnn>; Fri, 15 Dec 2006 16:00:42 +0300 (MSK)
        (envelope-from fnn@starttelecom.ru)
Received: from mail1.wimax.ru (mail1.wimax.ru [81.16.112.3])
        by aihs.fnn.ru (8.13.3/8.13.3) with ESMTP id kBFD0bU6010332
        for <fnn@fnn.ru>; Fri, 15 Dec 2006 14:00:38 +0100 (CET)
        (envelope-from fnn@starttelecom.ru)
Received: from [83.222.198.130] (account n.fedotov@starttelecom.ru
HELO fnn.starttelecom.ru)
  by mail1.wimax.ru (CommuniGate Pro SMTP 5.0.9)
  with ESMTPSA id 952840 for fnn@fnn.ru; Fri, 15 Dec 2006 16:00:37
+0300
From: Nikolay Nikolaevich Fedotov <fnn@starttelecom.ru>
Organization: Start-Telecom
To: fnn@fnn.ru
Subject: Path test
Date: Fri, 15 Dec 2006 16:00:05 +0300
User-Agent: KMail/1.9.4
MIME-Version: 1.0
Content-Type: text/plain;
  charset="koi8-r"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
Message-Id: <200612151600.05273.fnn@starttelecom.ru>

path test
--
Nikolay N Fedotov
Information Security Officer
Start Telecom Inc. (Russia)
```

Письмо в архиве входящей почты получателя:

```
From fnn@starttelecom.ru Fri Dec 15 16:00:43 2006
Return-Path: <fnn@starttelecom.ru>
Received: from aihs.fnn.ru (aihs-tun [10.5.0.1])
        by home.fnn.ru (8.13.1/8.13.1) with ESMTP id kBFD0g7M018585
        for <fnn@home.fnn>; Fri, 15 Dec 2006 16:00:42 +0300 (MSK)
        (envelope-from fnn@starttelecom.ru)
```

```
Received: from mail1.wimax.ru (mail1.wimax.ru [81.16.112.3])
        by aihs.fnn.ru (8.13.3/8.13.3) with ESMTP id kBFD0bU6010332
        for <fnn@fnn.ru>; Fri, 15 Dec 2006 14:00:38 +0100 (CET)
        (envelope-from fnn@starttelecom.ru)
Received: from [83.222.198.130] (account n.fedotov@starttelecom.ru
HELO fnn.starttelecom.ru)
  by mail1.wimax.ru (CommuniGate Pro SMTP 5.0.9)
  with ESMTPSA id 952840 for fnn@fnn.ru; Fri, 15 Dec 2006 16:00:37
+0300
From: Nikolay Nikolaevich Fedotov <fnn@starttelecom.ru>
Organization: Start-Telecom
To: fnn@fnn.ru
Subject: Path test
Date: Fri, 15 Dec 2006 16:00:05 +0300
User-Agent: KMail/1.9.4
MIME-Version: 1.0
Content-Type: text/plain;
  charset="koi8-r"
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
Message-Id: <200612151600.05273.fnn@starttelecom.ru>


path test
--
Nikolay N Fedotov
Information Security Officer
Start Telecom Inc. (Russia)
```

Дотошный читатель может самостоятельно сравнить отправленное и полученное сообщение и определить, какие именно служебные заголовки (кроме упоминавшихся маршрутных заголовков «Received») у них отличаются. Также можно сравнить указанные в логах и заголовках моменты времени и сделать из них выводы не только о «скорости» письма, но и о разнице в показаниях часов всех участвующих компьютеров.

Как видно по иллюстрациям, по пути к сообщению добавились три маршрутных заголовка «Received» соответственно трем серверам электронной почты (MTA), через которые сообщение прошло. Эти заголовки добавляются сверху, то есть нижний из них – первый, верхний – последний.

Бывает, что сервер добавляет не один, а два или даже три заголовка, если он производит какую-либо дополнительную, «внутреннюю» обработку или пересылку сообщения, например, передает его на проверку антивирусной программе. Приведем в качестве примера такого случая заголовки другого сообщения, полученного автором (тело сообщения не приводится).


```
From crackpotsaugur's@accion.org Wed Dec 13 02:25:42 2006
Return-Path: <crackpotsaugur's@accion.org>
Received: from aihs.fnn.ru (aihs-tun [10.5.0.1])
        by home.fnn.ru (8.13.1/8.13.1) with ESMTP id kBCNPfIu006292
        for <fnn@home.fnn>; Wed, 13 Dec 2006 02:25:41 +0300 (MSK)
        (envelope-from crackpotsaugur's@accion.org)
Received: from msk-m10-st01.rtcomm.ru (msk-m10-st01.rtcomm.ru
[213.59.0.34])
        by aihs.fnn.ru (8.13.3/8.13.3) with ESMTP id kBCNPb2X094397
        for <nfnn@fnn.ru>; Wed, 13 Dec 2006 00:25:38 +0100 (CET)
        (envelope-from crackpotsaugur's@accion.org)
Received: from msk-m10-st01.rtcomm.ru (localhost.rtcomm.ru
[127.0.0.1])
        by msk-m10-st01.rtcomm.ru (Postfix) with SMTP id D2E6669E19
        for <nfnn@fnn.ru>; Wed, 13 Dec 2006 02:25:37 +0300 (MSK)
Received: from p54BE5FBF.dip.t-dialin.net (p54BE5FBF.dip.t-
dialin.net [84.190.95.191])
        by msk-m10-st01.rtcomm.ru (Postfix) with ESMTP id
EB48069ED9
        for <nfnn@fnn.ru>; Wed, 13 Dec 2006 02:25:35 +0300 (MSK)
Received: from 12.15.162.211 (HELO smtp2.accion.org)
     by fnn.ru with esmtp (7(6.6-74)?F/ 4.43)
     id 58T.)?-.A-TUD-DX
     for nfnn@fnn.ru; Thu, 1 Jan 1998 11:05:44 -0060
From: "Juana Deal" <crackpotsaugur's@accion.org>
To: <nfnn@fnn.ru>
Subject: [!! SPAM] It ready
Date: Thu, 1 Jan 1998 11:05:44 -0060
Message-ID: <01bd16a5$34c829f0$6c822ecf@crackpotsaugur's>
MIME-Version: 1.0
Content-Type: text/plain;
        charset="iso-8859-2"
Content-Transfer-Encoding: 7bit
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Office Outlook, Build 11.0.5510
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2905
Thread-Index: Aca6Q,IL*A82<@Y=XJD'59Q+16@.**==
X-SpamTest-Envelope-From: crackpotsaugur's@accion.org
X-SpamTest-Group-ID: 00000000
X-SpamTest-Info: Profiles 597 [Dec 12 2006]
X-SpamTest-Info: {Headers: Spam A269}
X-SpamTest-Method: headers plus
X-SpamTest-Rate: 100
X-SpamTest-Status: SPAM
X-SpamTest-Status-Extended: spam
X-SpamTest-Version: SMTP-Filter Version 3.0.0 [0255], KAS30/Release
X-Anti-Virus: Kaspersky Anti-Virus for MailServers 5.5.2/RELEASE,
bases: 12122006 #236282, status:
notchecked
```

Два заголовка «`Received`» от одного и того же сервера (2-й и 3-й снизу) означают, что сообщение было обработано в два этапа: сначала принято, потом проверено антивирусно-антиспамовой программой и лишь после этого отослано дальше. При указанной проверке к служебным заголовкам были добавлены еще несколько заголовков, начинающиеся с «`X-SpamTest`».

Можно ли доверять заголовкам?

Возникает резонный вопрос: насколько сложно фальсифицировать служебные заголовки письма? Например, чтобы направить следствие по ложному пути.

Понятно, что, имея доступ на запись к лог-файлам и к архиву почты, можно изменить любые данные. А что можно фальсифицировать, не имея такого доступа?

Заголовки «`From`», «`To`», «`Subject`», «`Date`» и некоторые другие проставляются клиентской программой (MUA) отправителя и при дальнейшей передаче не изменяются. Поэтому отправитель может их заполнить по собственному усмотрению. Если клиентская программа этого сделать не позволяет, надо использовать другую программу или даже обойтись вовсе без нее, составив сообщение в любом текстовом редакторе и передав серверу через telnet. То есть заголовкам «`From`», «`To`», «`Date`» и «`Reply-To`» доверять нельзя.

Заголовок «`Return-Path`» проставляется принимающим сервером электронной почты, но его содержимое извлекается из команды «`mail from`», которую отдает клиентская сторона во время сеанса связи (SMTP-сессии). Соответственно, этот заголовок тоже может быть фальсифицирован.

Заголовки «`Received`» проставляются принимающим сервером. Поэтому передающая сторона подставить в них произвольные данные не может. Однако фальсификатор может поставить в передаваемое сообщение несколько подложных «`Received`», как будто сообщение уже ранее прошло через некие сервера. При получении сервер не проверяет соответствия последнего маршрутного заголовка «`Received`» и адреса передающего узла, поэтому такая подмена возможна. Однако последующие маршрутные заголовки будут добавляться уже вне контроля фальсификатора. Таким образом, можно доверять тому заголовку, который добавлен явно независимым, не находящимся под контролем злоумышленника сервером, а также всем последующим. Прочие заголовки «`Received`» следует проверять, сверяя их с записями в логах соответствующих серверов электронной почты.

Пример подложного заголовка можно увидеть на последней из иллюстраций в предыдущем параграфе. Первый (самый нижний) заголовок «`Received: from 12.15.162.211 (HELO smtp2.accion.org) by fnn.ru...`» явно подложный, поскольку проставлен он от имени несуществующего сервера «`fnn.ru`» из домена, который принадлежит получателю. Это довольно распространенная уловка для рассылки спама*.

Формат сообщений

Сообщения электронной почты имеют многовариантный, неоднократно расширявшийся формат, который определяется соответствующим стандартом [31].

В качестве приложений допустимы различные типы данных, в том числе произвольные, бинарные. При отправке и получении сообщений электронной почты клиентские программы стараются кодировать и декодировать данные без участия и ведома пользователя. Хранящийся в архиве исходный текст сообщения (см. примеры выше) часто совсем не похож на то, что видно в почтовом клиенте.

Содержимое тела сообщения и приложений может кодироваться несколькими различными способами: UUENCODE, Base64, quoted-printable. Оно может быть в обычном, текстовом формате, в HTML-формате или в обоих сразу.

В рамках данной книги невозможно описать всего разнообразия контента электронной почты, поэтому отошлем читателя к соответствующей литературе [2, 23, 31].

Документирование прохождения сообщений

В рамках предварительного следствия необходимо не только исследовать электронные следы с целью установления истины, но и добывать пригодные доказательства. То есть документировать действия в порядке, установленном УПК.

Предположим, в рамках расследования необходимо доказать факт направления сообщения электронной почты от подозреваемого к потерпевшему. Какие доказательства необходимо собрать для этого и как их закрепить? Автор предлагает три варианта – нестрогий, промежуточный и строгий.

Деревенский вариант

Производится осмотр или экспертиза компьютера отправителя. Из архива отправленных извлекается, распечатывается и приобщается к делу интересующее нас сообщение.

Производится осмотр или экспертиза компьютера получателя. Из архива полученных извлекается, распечатывается и приобщается к делу интересующее нас сообщение.

Оба вышеуказанных сообщения сравниваются. Должны совпасть тело письма (возможно, с точностью до кодировки) и основные служебные заголовки. Из этого совпадения делается вывод о том, что сообщение реально было отправлено и получено.

Провинциальный вариант

В дополнение к копиям сообщения с компьютеров отправителя и получателя к делу приобщается также документ о логах хотя бы одного сервера электронной почты (MTA), через который сообщение прошло, – протокол осмотра, заключение эксперта или, в крайнем случае, письменный ответ провайдера на запрос. Сервер должен находиться под управлением незаинтересованного лица, обычно это оператор связи. Данные из лога должны коррелировать с заголовками из полученного сообщения.

Таким образом, в лице независимого сервера появляется третья «точка опоры».

Столичный вариант

В деле должно иметься не менее трех независимых друг от друга свидетельств о прохождении письма. Например, компьютер отправителя, компьютер получателя и MTA провайдера. Либо компьютер получателя и MTA двух «промежуточных» провайдеров. Каждое должно быть закреплено экспертизой. Естественно, данные должны коррелировать.

Анонимные ремейлеры

Анонимизирующие транзитные сервера электронной почты – ремейлеры – предназначены для сокрытия отправителей сообщений, которые, согласно официальной политике этих серверов, «могут опасаться незаконных преследований или политических репрессий». Рассылка спама* через такой ремейлер невозможна – для этого предприняты соответствующие технические меры.

Пользователь отправляет сообщение на специальный адрес. Ремейлер получает его, расшифровывает, обрабатывает предусмотренным образом и затем отсылает на адрес, указанный пользователем в специальной команде в теле письма.

Функциональность и особенности хороших ремейлеров на сегодняшний день таковы:

- прием почты только в зашифрованном виде (с сильной криптографией);
- удаление всех без исключения служебных заголовков исходного письма;
- удаление всех других идентифицирующих признаков исходного письма;
- возможность вставлять произвольные заголовки;
- возможность задавать произвольную задержку в отправке;

- возможность «холостых» писем;
- возможность выстраивать цепочки из ремейлеров;
- гарантии отсутствия логов;
- расположение ремейлера в стране с либеральным законодательством;
- использование SMTP/TLS с соответствующими сертификатами;
- письма с приложениями (аттачами);
- использование отправителем обычного ПО, без каких-либо добавлений;
- встроенный антивирус.

Как правило, всё взаимодействие пользователя с ремейлером производится по электронной почте при помощи сообщений. Веб-сайты есть не у всех анонимайзеров, ибо наличие веб-сайта снижает анонимность.

В основном ремейлеры построены на программном обеспечении двух типов: «Cypherpunk» и «Mixmaster». Оба кода являются открытыми проектами.

Помимо описанных «канонических» ремейлеров существует великое множество коммерческих проектов на основе проприетарного ПО для анонимизации отправки электронной почты и других действий пользователей. Подписка на такие услуги обходится пользователю от 2 до 20 долларов ежемесячно. Как правило, требуется установить на рабочей станции пользователя программное обеспечение, которое взаимодействует с сервером и обеспечивает проксирование трафика.

Довольно часто подобные сервисы представляют собой заурядный обман потребителей, то есть они как-то работают, но анонимности не обеспечивают. Владельцев таких сервисов можно понять. Кому же захочется выглядеть перед властями соучастником и укрывателем террористов, хакеров, спамеров и прочих правонарушителей, да еще за такие смешные деньги?

История знает несколько случаев, когда владельцы анонимизирующих ремейлеров, несмотря на декларации об отсутствии логов, все же предоставляли властям сведения об IP-адресах отправителей. В некоторых странах попросту запрещено не вести логов или не сохранять их в течение положенного времени, например, в США. В таких странах настоящий анонимизирующий ремейлер работать не может. Но во многих странах законодательство довольно либерально и вполне позволяет предоставлять подобный сервис и не вести логи.

Некоторые анонимизирующие провайдеры (как, впрочем, и иные провайдеры) склонны сотрудничать с правоохранительными органами в деле установления личности своих клиентов, некоторые – нет. Сказать наперед, предоставит ли информацию тот или иной оператор связи, нельзя. В одних странах операторы обязаны это делать и подлежат наказанию в случае отказа. В других странах операторы такой обязанности не имеют. Тем не менее бывает по-разному. В первом случае все равно можно получить от оператора отказ под благовидным предлогом. А во втором

случае оператор может «сдать» своего клиента, которому обещал анонимность, особенно если информацию запросит местная полиция, у которой свои собственные рычаги влияния. На что можно твердо надеяться – так это на то, что оператор прекратит предоставление услуг клиенту, замешанному в криминальной деятельности, поскольку это может отрицательно сказаться на самом операторе.

Установление принадлежности и расположения IP-адреса

Почти в каждом уголовном деле, связанном с сетью Интернет, присутствовала такая задача: по известному IP-адресу установить использующий его компьютер и местоположение этого компьютера.

Как правило, цепочка доказательств выглядит именно таким образом:

(преступление) – (IP-адрес) – (компьютер) – (человек)

При помощи различных технических средств фиксируется IP-адрес, с которого осуществлялась криминальная деятельность. Затем устанавливается компьютер, который использовал данный IP-адрес, факт такого использования закрепляется экспертизой. Затем следует доказать, что этим компьютером в соответствующее время управлял подозреваемый.

Вторая из упомянутых задач – найти компьютер по его IP-адресу – и будет предметом рассмотрения в данной главе.

Уникальность

IP-адрес является уникальным идентификатором компьютера или иного устройства в сети Интернет. Это значит, что в пределах всей глобальной компьютерной сети в каждый момент времени только один-единственный компьютер может использовать определенный IP-адрес. Из этого правила имеется целый ряд исключений:

- приватные*, или так называемые «серые» IP-адреса;
- коллективные, или мультикастовые (multicast) IP-адреса;
- сетевые и широковещательные (broadcast) IP-адреса;
- не выделенные или не присвоенные регистратором IP-адреса;
- IP-адреса, относящиеся к территориально распределенным кластерам компьютеров.

Если же IP-адрес относится к категории публичных* (так называемых «белых») адресов, если он должным образом выделен одним из регистраторов, то этот адрес будет маршрутизироваться. То есть IP-пакет, отправленный на этот адрес из любой точки Интернета, найдет свою цель. Это значит, что данный IP-адрес – уникальный. И возможно установить компьютер, которому принадлежит этот IP-адрес.

Является ли тот или иной IP-адрес уникальным, не принадлежит ли он к упомянутым исключениям – это устанавливает специалист или эксперт.

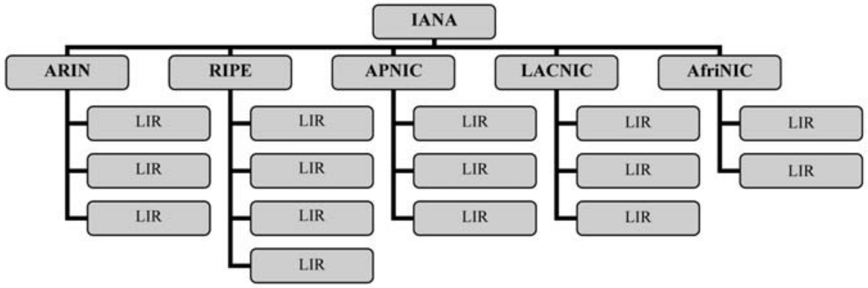
Регистраторы

Выделением и регистрацией IP-адресов в Интернете занимаются организации, именуемые регистраторами IP-адресов (IP Registry). Это организации, являющиеся органами самоуправления* Интернета.

Регистраторы образуют трехуровневую иерархию: IANA – RIR – LIR.

Организация IANA является главным регистратором, она выделяет самые крупные блоки IP-адресов региональным регистраторам и большим организациям.

Региональных регистраторов (RIR) в настоящее время пять. Это ARIN (Северная Америка), RIPE (Европа и Центральная Азия), APNIC (Азиатско-Тихоокеанский регион), LACNIC (Латинская Америка), AfriNIC (Африка). Они выделяют крупные и средние блоки адресов местным регистраторам (LIR), а также ведут базу данных выделенных IP-адресов и предоставляют доступ к ней.



Местные регистраторы (LIR) выделяют мелкие блоки IP-адресов операторам связи и потребителям и регистрируют их в базе данных своего регионального регистратора. Как правило, роль местного регистратора исполняет оператор связи (интернет-провайдер). Таких регистраторов – несколько тысяч.

Все выделенные IP-адреса регистрируются в специальной базе данных, которую поддерживает региональный регистратор (RIR). Сведения из этой базы данных (за исключением некоторых полей) доступны любому лицу по протоколу whois [22]. Обратиться к этой базе достаточно просто. При наличии доступа в Интернет надо набрать в командной строке «`whois <ip-адрес>`». Такая команда имеется в любой операционной системе, кроме Windows. Для тех, кому она недоступна или неудобна, есть многочисленные веб-интерфейсы, то есть веб-страницы, на которых можно ввести запрашиваемый IP-адрес и получить ответ из соответствующей базы данных при помощи браузера.

Установление принадлежности IP-адреса через whois-клиент

Давайте для примера попробуем установить, где живет в настоящее время известный экстремистский ресурс «Кавказ-центр». Определим соответствующий ему IP-адрес и спросим об этом IP-адресе регистратора RIPE. Команда «host» разрешает доменное имя в IP-адрес, а последующая команда «whois3» связывается с whois-сервером указанного регистратора, делает запрос к его базе данных и выводит на экран всю полученную информацию.

```
$>host www.kavkazcenter.com
www.kavkazcenter.com has address 88.80.5.42

$>whois3 -B 88.80.5.42
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
%
% Note: the default output of the RIPE Whois server
% is changed. Your tools may need to be adjusted. See
% http://www.ripe.net/db/news/abuse-proposal-20050331.html
% for more details.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

% Information related to '88.80.2.0 - 88.80.7.255'

inetnum:        88.80.2.0 - 88.80.7.255
netname:        PRQ-NET-COLO
descr:          prq Inet POP STH3
descr:          Co-located customer servers
country:        SE
admin-c:        pIN7-RIPE
tech-c:         pIN7-RIPE
status:         ASSIGNED PA
notify:         registry-ripenotify@prq.se
mnt-by:         MNT-PRQ
changed:        registry-ripe@prq.se 20051125
source:         RIPE

role:           prq Inet NOC
address:        prq Inet
                 Box 1206
                 SE 11479 Stockholm
                 Sweden
phone:          +46 (0)8 50003150
e-mail:         noc@prq.se
e-mail:         registry-ripe@prq.se
remarks:       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
remarks:       ! Abuse reports should ONLY be sent to abuse@prq.se !
remarks:       ! Do NOT call unless it's very urgent               !
remarks:       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
admin-c:        PW1115-RIPE
```



```
admin-c:        AC9661-RIPE
tech-c:         PW1115-RIPE
tech-c:         AC9661-RIPE
nic-hdl:        pIN7-RIPE
mnt-by:         MNT-PRQ
changed:        registry-ripe@prq.se 20040707
changed:        registry-ripe@prq.se 20050802
changed:        registry-ripe@prq.se 20060308
changed:        registry-ripe@prq.se 20060324
changed:        registry-ripe@prq.se 20060508
source:         RIPE
abuse-mailbox:  abuse@prq.se

% Information related to '88.80.0.0/19AS33837'

route:          88.80.0.0/19
descr:          prq Inet aggregated route
origin:         AS33837
notify:         registry-ripenotify@prq.se
mnt-by:         MNT-PRQ
changed:        registry-ripe@prq.se 20051124
source:         RIPE
```

Из полученного ответа усматривается, что диапазон IP-адресов с 88.80.0.0 по 88.80.31.255 выделен шведскому оператору связи «prq Inet». Из этого диапазона меньший поддиапазон с 88.80.2.0 по 88.80.7.255 используется как «Co-located customer servers», то есть для клиентских серверов на колокации*. В их числе и интересующий нас 88.80.5.42 (www.kavkazcenter.com).

«Соседями» домена «www.kavkazcenter.com», то есть доменами, имеющими тот же IP-адрес, оказались, согласно данным проекта «IP Neighbors Domain Check» [W06], следующие:

```
kavkaz.org.uk
kavkaz.tv
kavkaz.uk.com
kavkazcenter.com
kavkazcenter.info
kavkazcenter.net
old.kavkazcenter.com
pda.kavkaz.tv
pda.kavkazcenter.com
wap.kavkaz.tv
```

Из чего можно заключить, что на этом сервере живут только проекты одного клиента. Это значит, что сервер – выделенный, принадлежит клиенту или целиком арендуется им у провайдера.

Установление принадлежности IP-адреса через веб-форму

Тот же результат можно получить, сделав запрос через веб-форму на веб-сайте RIPE – Европейского регистратора IP-адресов или каком-либо другом веб-сайте, имеющем аналогичную функцию.

Разница между получением справки через whois-клиент и веб-форму невелика. Источник тот же. Просто во втором случае добавляется еще один технический посредник в лице чужого веб-сайта.

Запрос whois-сервера через веб-форму

Корректность

Можно ли доверять данным, полученным таким способом? Обязанности по внесению, изменению и удалению записей лежат на местных регистраторах (LIR). Но за исполнением этих обязанностей строго не следят. Местный регистратор может несвоевременно обновить запись или же, чтобы облегчить себе работу, зарегистрировать одной записью диапазон адресов, выделенных нескольким разным клиентам. Кроме того, данные о пользователях IP-адресов заносятся, как правило, со слов клиента, без должной верификации. Всё это приводит к тому, что среди записей указанной базы данных встречаются неверные – устаревшие или с неполными, некорректными сведениями.

Поэтому всецело доверять таким сведениям не следует. Как правило, сведения о местном регистраторе (LIR) – верные, поскольку LIR является членом регионального регистратора (RIR), имеет с ним договор, платит членские взносы, постоянно взаимодействует. А сведения о клиенте LIR'a, непосредственном пользователе IP, подлежат дальнейшей проверке.

Трассировка IP-адреса

Также некоторую помощь в установлении местоположения и принадлежности IP-адреса может оказать программа «`traceroute`», которая имеется в составе любой операционной системы, даже Windows.

Принцип действия этой программы таков. С компьютера исследователя испускаются IP-пакеты, адресованные на целевой IP-адрес. Обычно это пакеты протокола UDP, но можно использовать и любой другой. Поле TTL каждого испущенного пакета выставляется последовательно равным 1, 2, 3 и так далее. Это поле предназначено для исключения перегрузки каналов на случай образования петель маршрутизации, то есть замкнутых маршрутов. При прохождении каждого маршрутизатора (маршрутизирующего устройства) поле TTL уменьшается на единицу. При достижении значения 0 этот IP-пакет сбрасывается, а в адрес отправителя посылается специальное уведомление – сообщение протокола ICMP [80], тип 11, код 0. Следовательно, пакет с TTL=1 будет сброшен на первом маршрутизаторе по пути следования, пакет с TTL=2 – на втором маршрутизаторе и так далее. По обратному адресу принятых ICMP-пакетов компьютер исследователя устанавливает, через какие узлы пролегает маршрут до целевого компьютера.

Вот пример работы программы «`traceroute`». Попробуем с ее помощью определить, где располагается сервер `www.microsoft.com`.

```
$>traceroute www.microsoft.com
traceroute: Warning: www.microsoft.com has multiple addresses; using
207.46.18.30
traceroute to lb1.www.ms.akadns.net (207.46.18.30), 64 hops max, 40
byte packets
 1  gw.mkfinance.ru (10.0.4.61)  0.264 ms  0.238 ms  0.281 ms
 2  D1-MCH-gi0-2.80.rusmedia.net (83.222.194.1)  63.927 ms  48.689
ms *
 3  C1-M9-gi1-3-0.3.rusmedia.net (212.69.98.229)  26.845 ms  48.375
ms  21.793 ms
 4  msk-dsr5-vl305.rt-comm.ru (195.161.4.153)  36.798 ms  64.589 ms
79.828 ms
 5  195.50.92.1 (195.50.92.1)  111.559 ms  125.433 ms  123.118 ms
 6  ae-0-56.bbr2.London1.Level3.net (4.68.116.162)  93.407 ms ae-0-
52.bbr2.London1.Level3.net (4.68.116.34)  200.311 ms  100.872 ms
 7  as-0-0.bbr1.SanJose1.Level3.net (64.159.1.133)  253.125 ms ae-0-
0.bbr2.SanJose1.Level3.net (64.159.1.130)  258.511 ms as-0-
0.bbr1.SanJose1.Level3.net (64.159.1.133)  445.133 ms
 8  ge-4-0-0-56.gar1.SanJose1.Level3.net (4.68.123.162)  248.892 ms
ge-2-0-0-51.gar1.SanJose1.Level3.net (4.68.123.2)  348.158 ms ge-4-
0-0-52.gar1.SanJose1.Level3.net (4.68.123.34)  318.136 ms
 9  MICROSOFT-C.gar1.SanJose1.Level3.net (209.245.144.110)  229.556
ms  338.955 ms  234.984 ms
10  ge-7-3-0-45.sjc-64cb-1b.ntwk.msn.net (207.46.45.35)  289.415 ms
253.833 ms  245.386 ms
11  ten9-2.bay-76c-1b.ntwk.msn.net (207.46.37.166)  253.875 ms
383.844 ms  355.371 ms
12  ten8-3.bay-76c-1d.ntwk.msn.net (64.4.63.2)  310.604 ms  245.782
ms  273.315 ms
13  po33.bay-6nf-mcs-3b.ntwk.msn.net (64.4.63.90)  245.387 ms
```

```
260.270 ms  257.520 ms
14  * po33.bay-6nf-mcs-3b.ntwk.msn.net (64.4.63.90)  297.405 ms !X *
15  po33.bay-6nf-mcs-3b.ntwk.msn.net (64.4.63.90)  251.177 ms !X *
440.829 ms !X
```

Как видим, пакеты шли через узлы провайдера «`rusmedia.net`» (шаги 2 и 3), затем через «`rt-comm.ru`» (шаг 4), потом через «`level3.net`» (6-9). На девятом шаге пакет, очевидно, перешел в сеть «Майкрософт», потому что соответствующий маршрутизатор имеет в своем имени «microsoft», хотя это имя в домене «level3.net». Все прочие шаги – внутри корпоративной сети Майкрософта (msn.net). В именах транзитных маршрутизаторов мы можем заметить названия «msk» (Москва), «london» (Лондон) «sanjose» (Сан-Хосе) – это дает представление об их физическом расположении. Финальный сервер, скорее всего, тоже стоит в городе Сан-Хосе.

Попробуем трассировать тот же сервер из другого места Интернета.

```
fnn@home$>traceroute 207.46.18.30
traceroute to 207.46.18.30 (207.46.18.30), 64 hops max, 40 byte
packets
 1  aihs-tun (10.5.0.1)  81.374 ms  77.511 ms  117.574 ms
 2  bg-aihs.net (80.94.80.1)  101.864 ms  106.277 ms  63.229 ms
 3  v283.mpd01.fra03.atlas.cogentco.com (149.6.81.37)  227.850 ms
267.295 ms  221.259 ms
 4  t13-0-0.core01.fra03.atlas.cogentco.com (130.117.1.221)  93.270
ms  113.874 ms  88.356 ms
 5  t4-3.mpd01.fra03.atlas.cogentco.com (130.117.0.246)  180.930 ms
188.143 ms  179.462 ms
 6  t4-1.mpd01.par02.atlas.cogentco.com (130.117.2.14)  183.689 ms
176.424 ms  167.548 ms
 7  t2-2.mpd02.par01.atlas.cogentco.com (130.117.2.81)  175.570 ms
170.390 ms  178.438 ms
 8  g5-1.mpd01.par01.atlas.cogentco.com (130.117.2.49)  205.371 ms
190.409 ms  170.393 ms
 9  p14-0.core01.jfk02.atlas.cogentco.com (130.117.1.245)  158.309
ms  164.527 ms  164.132 ms
10  p4-0.core02.dca01.atlas.cogentco.com (66.28.4.81)  163.937 ms
167.115 ms  167.780 ms
11  t4-3.mpd01.dca01.atlas.cogentco.com (154.54.5.57)  171.609 ms
174.707 ms  187.524 ms
12  v3498.mpd01.dca02.atlas.cogentco.com (154.54.7.6)  173.299 ms
172.891 ms  180.584 ms
13  t2-2.mpd01.iad01.atlas.cogentco.com (154.54.1.78)  174.717 ms
176.820 ms  244.616 ms
14  ge5-1.edge1.ash1.us.msn.net (154.54.10.102)  167.459 ms  181.929
ms  181.873 ms
15  207.46.47.92 (207.46.47.92)  179.655 ms  170.900 ms  202.355 ms
16  so-6-0-0-0.pao-64cb-1a.ntwk.msn.net (207.46.33.61)  242.773 ms
303.281 ms  326.135 ms
17  * ten9-2.bay-76c-1c.ntwk.msn.net (207.46.37.161)  272.496 ms
259.461 ms
```



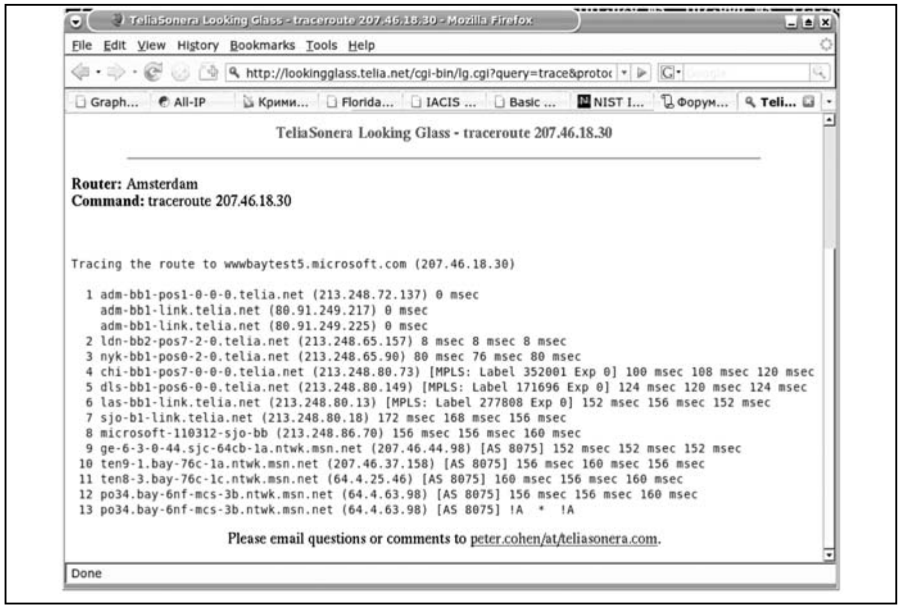
```
18  po34.bay-6nf-mcs-3b.ntwk.msn.net (64.4.63.98)  247.020 ms
250.746 ms  291.349 ms
19  po34.bay-6nf-mcs-3b.ntwk.msn.net (64.4.63.98)  339.056 ms !X *
242.941 ms !X
fnn@home$>
```

Путь пакетов пролегает через провайдера «Cogent Communications, Inc.» (`cogentco.com`), откуда непосредственно переходит в корпоративную сеть «Майкрософта» (`msn.net`).

Кроме IP-адресов установленных в ходе трассировки узлов указаны соответствующие им доменные имена. Среди операторов связи принято назначать маршрутизаторам доменные имена, говорящие об их принадлежности и географическом расположении. Поэтому можно приблизительно судить о местоположении и подключении целевого адреса. В показанном примере в именах маршрутизаторов мы видим метки городов: «fra» (Франкфурт-на-Майне), «par» (Париж), «jfk» (Нью-Йорк), «dca» (Вашингтон), «iad» (Вашингтон), «ash» (Эшбурн), «pao» (Пало-Альто). Эти метки-аббревиатуры взяты из кодов аэропортов соответствующих городов.

Иногда полезно трассировать искомый адрес из разных точек Сети, как бы с разных сторон, чтобы получить более надежные сведения. Для этого можно воспользоваться многочисленными публичными сервисами «looking glass», которые установлены у разных провайдеров и доступны через веб-формы.

Попробуем трассировать тот же адрес из третьей точки при помощи такого инструмента.

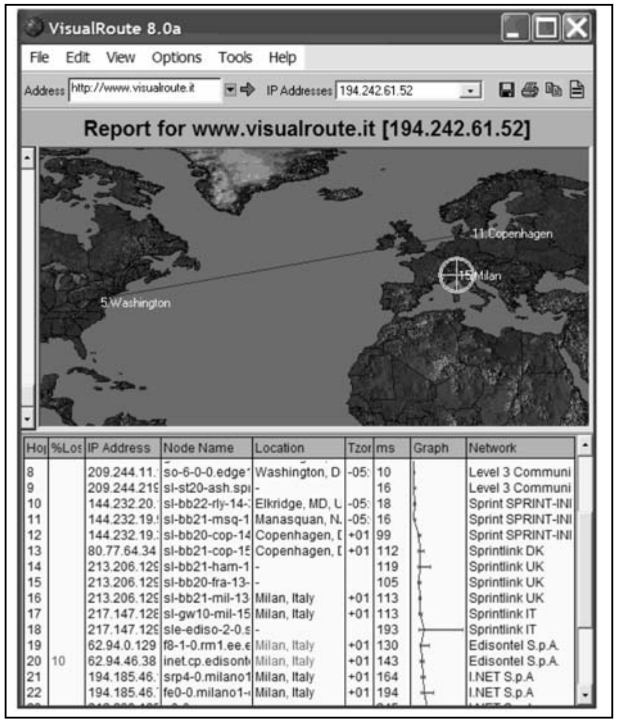


Веб-интерфейс для трассировки адреса с узла провайдера («looking glass»)

Путь пакета обозначается кодами: adm (Амстердам), ldn (Лондон), nyk (Нью-Йорк), chi (Чикаго), dls (Даллас), las (Лос-Анджелес), sjo (Сан-Хосе).

В этом случае сети «Телии» и «Майкрософта», очевидно, стыкуются в Сан-Хосе (код «sjo», см. шаги 7-8).

У каждого провайдера свои принципы наименования маршрутизаторов и свои условные обозначения. Тем не менее все стараются придерживаться определенных правил и использовать понятные мнемоники [W25]. В случае неясности можно попробовать посмотреть whois-запись для соответствующего IP-адреса, в ней также можно найти указание на географическое расположение.



Визуальный трассировщик IP-адреса

Операции по анализу результатов трассировки IP-адреса, их сопоставлению с географией частично поддаются автоматизации. Есть несколько программ, которые с большим или меньшим успехом идентифицируют промежуточные узлы в трассировке.

К сожалению, нельзя полностью доверять доменным именам узлов, которые определяются программой «`traceroute`». Следить за корректностью этих имен провайдеры не обязаны. Так что результаты трассировки могут служить лишь косвенным указанием на местоположение компьютера.

Кроме того, «`traceroute`», работая исключительно на 3-м (сетевом) уровне, не видит туннели, VPN, MPLS и некоторые иные особенности организации сети. В качестве иллюстрации читателю предлагается самостоятельно попробовать определить при помощи трассировки географическое местоположение домашнего компьютера автора «`home.fnn.ru`».

Неуловимый IP

Приведем еще один интересный пример. Это «зомби-хостинг», то есть содержание публичных сетевых ресурсов не на серверах, а на компьютерах зомби-сети* (ботнета). Зомбированные клиентские компьютеры используются как в качестве веб-серверов, так и в качестве DNS-серверов для соответствующего домена [23]. Зомби-сервер живет недолго – от нескольких часов до нескольких дней. Однако их много. Поэтому можно поддерживать постоянную доступность.

Ниже приводятся результаты проделанного автором эксперимента. В листинге показаны результаты запросов относительно NS-серверов и IP-адреса для доменного имени «send-safe.com», это веб-сайт широко известного в узких кругах производителя программного обеспечения для рассылки спама*. Сделаем несколько DNS-запросов с интервалом в пять минут:

```
fnn@home$>host -t ns send-safe.com
send-safe.com name server ns3.safe4net.net.
send-safe.com name server ns4.safe4net.net.
send-safe.com name server ns1.safe4net.net.
send-safe.com name server ns2.safe4net.net.
fnn@home$>host -t ns send-safe.com
send-safe.com name server ns1.london2portal.com.
send-safe.com name server ns2.london2portal.com.
fnn@home$>host send-safe.com
send-safe.com has address 89.36.47.10
send-safe.com has address 89.78.70.224
send-safe.com has address 68.37.246.232
send-safe.com has address 69.155.132.152
send-safe.com has address 71.155.241.20
fnn@home$>host send-safe.com
send-safe.com has address 86.20.204.169
send-safe.com has address 213.85.5.23
send-safe.com has address 66.61.23.171
send-safe.com has address 81.106.163.50
send-safe.com has address 82.138.37.213
fnn@home$>host send-safe.com
send-safe.com has address 24.9.184.225
send-safe.com has address 71.60.68.225
send-safe.com has address 71.155.241.20
send-safe.com has address 212.1.227.1
send-safe.com has address 217.173.174.237
fnn@home$>host send-safe.com
send-safe.com has address 24.9.184.225
```

```
send-safe.com has address 71.60.68.225
send-safe.com has address 82.246.189.246
send-safe.com has address 87.240.24.61
send-safe.com has address 212.1.227.1
fnn@home$>host send-safe.com
send-safe.com has address 66.61.23.171
send-safe.com has address 71.155.241.20
send-safe.com has address 82.138.37.213
send-safe.com has address 86.20.204.169
send-safe.com has address 213.85.5.23
```

Как видно, NS-сервера довольно часто меняются. Меняются и IP-адреса веб-сайта, причем в каждый момент их доступно несколько. То есть веб-сайт и обслуживающие его DNS-сервера рассредоточены и постоянно мигрируют. Если начать наводить справки о принадлежности и географическом положении всех выявленных IP-адресов, то окажется, что они равномерно разбросаны по всему Интернету. На самом деле это адреса зомбированных компьютеров, пригодных для размещения веб-сайтов. То есть веб-сайт как бы «размазан» по большой зомби-сети*. Благодаря такой технологии веб-сайт «`send-safe.com`» виден пользователям с очень высокой вероятностью, однако прекратить его работу весьма затруднительно.

Зафиксировать положение такого сайта невозможно, обнаружить его владельца довольно трудно, доказать факт управления таким сайтом-призраком тоже нелегко.

Описанная технология применяется довольно редко. Подавляющее же большинство веб-сайтов живут на фиксированных IP-адресах, операторы-владельцы которых знают если не о личности владельца сайта, то, по крайней мере, о самом факте размещения.

Пространство и время

IP-адреса могут переходить от одного пользователя к другому. Некоторые из них выделяются на постоянной основе – они именуются статическими. Другие же IP-адреса выделяются только на конкретный сеанс связи и называются динамическими. Для статических IP-адресов период жизни исчисляется месяцами и годами, а для динамических – минутами.

В записях для тех диапазонов IP-адресов, которые используются для динамического выделения, обычно это указывается. Там можно увидеть слова «dynamic», «dialup» или «NAT».

В обоих случаях при установлении принадлежности IP-адресов следует учитывать момент времени, по состоянию на который мы хотим установить пользователя этого адреса. Для динамических IP-адресов этот момент надо указывать с точностью до секунды, поскольку бывают совсем короткие сеансы связи. Кроме времени следует указать часовой пояс и возможную погрешность часов, по которым фиксировалось время.

Документирование

Для уголовного дела, скорее всего, будет недостаточно простой распечатки ответа whois-сервера. Получить же официальную справку от европейского регионального регистратора RIPE будет весьма затруднительно, поскольку офис его находится в Амстердаме. Офисы других региональных регистраторов – еще дальше.

Нынешняя практика предусматривает два способа документирования ответа whois-сервера. Первый вариант: распечатка такого ответа может быть заверена каким-либо местным оператором связи, являющимся одновременно местным регистратором (LIR). В таком качестве часто выбирают РОСНИИРОС как старую и авторитетную организацию. Второй вариант: получение сведений о принадлежности IP-адреса оформляется рапортом оперуполномоченного; сведения из базы данных регистратора приводятся прямо в тексте рапорта. Иные варианты документирования (экспертиза, нотариальное заверение, справка от RIR) возможны, но до сих пор не применялись на практике.

Принадлежность IP-адреса к конкретному компьютеру все равно должна подтверждаться экспертизой этого компьютера и показаниями сотрудников оператора связи. Поэтому описанная нестрогость в документировании ответа whois-сервера вполне допустима.

Физическое расположение

Из данных регистратора мы узнаем, за кем закреплена соответствующая подсеть или диапазон IP-адресов. Обычно таковым субъектом является оператор связи или его клиент. Очень редко в базе данных регистратора значится непосредственный пользователь IP-адреса.

Получить или уточнить данные о непосредственном пользователе, а также установить его географическое расположение можно у оператора связи, на которого зарегистрирован соответствующий диапазон IP. Бывает, что этот оператор не знает точного местоположения клиента, поскольку между ним и клиентом находится оператор-посредник или оператор последней мили. Бывает, что посредник не единственный. В таком случае придется пройти по всей цепочке операторов.

В принципе, функция определения местоположения конечного оборудования (компьютера пользователя) предусмотрена в СОРМе. Однако очень мало надежды, что такая функция в действительности работает в силу того, что операторы связи учитывают своих клиентов по-разному, держат эти данные в самых различных форматах и редко организуют к ним онлайновый доступ для ФСБ. Привести весь клиентский учет всех операторов к единому знаменателю – задача на сегодняшний день невыполнимая.

Пример

Приведем характерный пример из практики.

Установлено, что неправомерный доступ к компьютерной информации был осуществлен 31.12.06, 21:01:30 по московскому времени с IP-адреса `217.107.0.58`. Данный адрес зафиксирован техническими средствами потерпевшего и его провайдера и закреплен протоколами осмотра и актом экспертизы.

Запрашиваем whois и выясняем, что сеть `217.107.0.0-217.107.255.255` зарегистрирована за провайдером «Главтелеком», а подсеть `217.107.0.0-217.107.0.255` – за провайдером «Урюпинский хостинг». Первой части этих данных можно верить, поскольку «Главтелеком» является LIR'ом и данные о нем заносятся в базу самим региональным регистратором (RIR). Вторая же часть данных вызывает немного меньше доверия, поскольку здесь выше вероятность ошибки, да и времени с момента последнего обновления записи прошло немало.

Соответствующую распечатку ответа whois-сервера оформляем рапортом оперативного сотрудника. А в «Главтелеком» направляем официальный запрос с требованием предоставить информацию о клиенте.

Получаем ответ, в котором ОАО «Главтелеком» подтверждает, что диапазон `217.107.0.0-217.107.0.255` на интересующий момент времени был выделен в пользование его клиенту – ЗАО «Урюпинский хостинг». О дальнейшем распределении и использовании этих IP-адресов знают только в Урюпинске.

Предполагая, что злоумышленником является не сотрудник этого провайдера, а его клиент, и считая провайдера лицом незаинтересованным, запрашиваем ЗАО «Урюпинский хостинг» об интересующем нас адресе `217.107.0.58`, указав точный момент времени, когда имел место неправомерный доступ.

Получаем ответ из Урюпинска, что поддиапазон адресов `217.107.0.2-217.107.0.63` используется для динамического выделения клиентам услуги коммутируемого доступа (dial-up), а в указанный момент (31.12.06, 18:01:30 по Гринвичу) этот адрес использовался клиентом, авторизованным по логину «pupkin». Этот логин, в свою очередь, закреплен за договором №163/2006 на имя Пупкиной Ирины Васильевны.

Для закрепления доказательств следует изъять и отправить на экспертизу компьютер, на котором функционировали технические средства, производившие авторизацию пользователя, выделение динамического IP-адреса и ведение соответствующих лог-файлов. Вместо изъятия и экспертизы можно ограничиться осмотром указанных компьютеров и лог-файлов (подробнее см. главу «Осмотр места происшествия»). Также следует изъять клиентский договор.

Окончательное закрепление доказательств производится в ходе экспертизы компьютера из квартиры Пупкина.

Итак, цепочка доказательств, привязывающая IP-адрес к компьютеру конечного пользователя, у нас сложилась такая:

- рапорт оперуполномоченного Иванова о выделении сети `217.107.0.0-217.107.255.255` российскому провайдеру «Главтелеком»;
- справка из «Главтелекома» о выделении сети `217.107.0.0-217.107.0.255` провайдеру «Урюпинский хостинг»;
- справка из ЗАО «У.Х.» об использовании подсети `217.107.0.2-217.107.0.63` для динамического выделения клиентам;
- протокол осмотра сервера «У.Х.», где в логах значится выделение адреса `217.107.0.58` пользователю **«pupkin»** в период 31.12.06, 22:45:31-23:20:12 по местному времени;
- клиентский договор, из которого следует принадлежность логина «pupkin»;
- акт экспертизы компьютера, изъятого при обыске в квартире Пупкина, где зафиксирован факт выхода в Интернет в период 31.12.06, 22:46:31-23:21:12 через модемный пул провайдера «У.Х.».

Цепочка замкнулась и защелкнулась. Некоторые особенности этой цепочки (вхождение одного диапазона IP в другой диапазон, особенности авторизации, разница и регулярное смещение временны́х интервалов и т.п.) может пояснить эксперт или специалист в ходе его допроса.

Прочее

Понятно, что невозможно не только изложить в данной книге, но даже просто упомянуть все возможные особенности и трудности в задаче установления принадлежности IP-адресов. Например, использование протокола IP версии 6 (все вышесказанное относится только к версии 4), трансляция IP-адресов, туннелирование, несимметричная маршрутизация, провайдер, не учитывающий или не знающий своих клиентов, использование прокси-серверов и иных посредников для сокрытия истинного IP-адреса и т.д.

Подобные препятствия встречаются сплошь и рядом. Описать все возможные случаи – означает изложить полное содержание нескольких учебных курсов. На освоение соответствующих знаний ИТ-специалист тратит годы, и было бы наивно полагать, что все это можно объяснить оперу, следователю или судье простыми словами за несколько часов.

Поэтому при установлении принадлежности и местоположения IP-адреса в ходе ОРМ или предварительного следствия участие технического специалиста обязательно.

Установление принадлежности доменного имени

Домен – область (ветвь) иерархического пространства доменных имен сети Интернет, которая обозначается уникальным доменным именем [L03].

Подробнее о доменных именах и их правовой природе можно прочесть в популярной книге А. Серго [25]. Здесь автор будет исходить из того, что читателю в общих чертах, то есть на уровне пользователя, известно, для чего предназначены и как используются доменные имена.

Некоторые юристы относят доменное имя к средствам индивидуализации (ст. 138 ГК). Другие не склонны считать его таковым и говорят, что юридическая природа доменного имени пока четко не определена. Есть даже экзотическое мнение, что доменные имена – это ресурс нумерации электросвязи (ст. 2 и 26 ФЗ «О связи»).

В отличие от юридической, техническая природа доменных имен известна хорошо и четко описана в соответствующих технических стандартах [26-29].

Для справедливого распределения пространства доменных имен и обеспечения их глобальной уникальности действует система регистрации доменных имен. Подлежат регистрации все доменные имена первого уровня (например, `org`, `info`, `ru`, `ua`), все доменные имена второго уровня (например, `gprf.info`, `fnn.ru`) и некоторые, выделенные доменные имена третьего уровня (например, `provider.net.ru`, `london.co.uk`). Прочие доменные имена регистрации не подлежат и распределяются по усмотрению владельца соответствующего домена более высокого уровня (например, домены `www.fnn.ru` и `mail.fnn.ru` создаются и используются исключительно по воле владельца домена второго уровня `fnn.ru`).

Для каждого домена, где предусмотрена обязательная регистрация, назначен регистратор или несколько регистраторов. В последнем случае все регистраторы обязаны использовать единую базу данных (централизованную или распределенную) для обеспечения уникальности регистрируемых доменных имен.

Все базы данных всех регистраторов являются публично доступными по протоколу whois, аналогично регистраторам IP-адресов.

Для домена ru регистраторов существует несколько (по состоянию на сегодня – 14). Они имеют централизованную базу данных, а кроме того – индивидуальные базы данных, являющиеся подмножеством центральной.

Таким образом, чтобы установить владельца какого-либо доменного имени из числа подлежащих регистрации, следует обратиться к базе данных соответствующего регистратора. Для не подлежащих регистрации доменных имен обращаться нужно к владельцу соответствующего домена более высокого уровня.

Например, нам требуется установить владельца доменного имени 3-го уровня «`www.internet-law.ru`». (Не путать с веб-сайтом, живущим на этом домене! Домен и веб-сайт иногда могут иметь разных владельцев.)

Очевидно, что данный домен 3-го уровня не относится к числу регистрируемых. Он находится в полном распоряжении владельца соответствующего домена 2-го уровня, то есть домена «`internet-law.ru`», который уже зарегистрирован.

Здесь придется сделать допущение (впоследствии, если понадобится, это надо будет подкрепить соответствующими доказательствами), а именно предположить, что указанный домен 3-го уровня в силу стандартности его имени (www) принадлежит тому же владельцу, что и домен 2-го уровня.

Чтобы узнать владельца доменного имени «`internet-law.ru`», обращаемся к базе данных российских регистраторов доменов. Для этого используем команду «`whois`», имеющуюся в любой ОС (кроме Windows). В качестве аргумента мы задаем искомое доменное имя, а параметр определяет, какой реестр запрашивать. Параметр «`-c ru`» указывает реестр доменных имен для России.

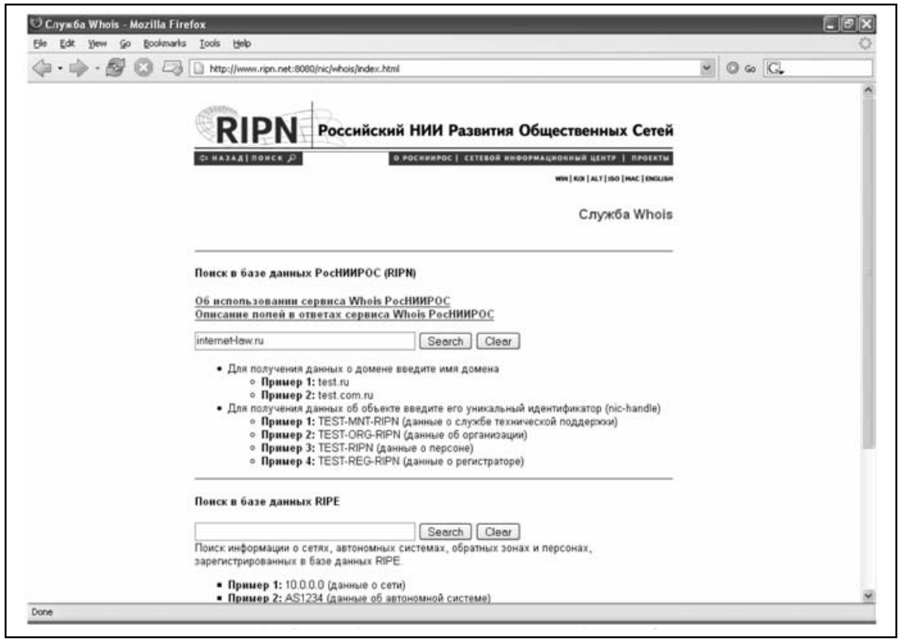
```
$>whois -c ru internet-law.ru
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

domain:      INTERNET-LAW.RU
type:        CORPORATE
nserver:     ns.masterhost.ru.
nserver:     ns1.masterhost.ru.
nserver:     ns2.masterhost.ru.
state:       REGISTERED, DELEGATED
org:         ANO "Internet & Law"
phone:       +7 495 7860130
e-mail:      mail@internet-law.ru
registrar:   RUCENTER-REG-RIPN
created:     2001.10.30
paid-till:   2007.10.30
source:      TC-RIPN

Last updated on 2006.12.16 14:02:58 MSK/MSD
```

Нам отвечает whois-сервер технического центра РОСНИИРОСа (TC-RIPN) – именно он поддерживает единую базу данных всех регистраторов в домене ru.

Ровно ту же самую информацию можно получить через веб-интерфейс, расположенный на веб-сайте РОСНИИРОСа (`http://www.ripn.net:8080/nic/whois/index.html`) или на многих других веб-сайтах.



Запрос доменного имени через веб-интерфейс

Ответ веб-интерфейса

Изучение ответа

Формат ответа устанавливается владельцем соответствующей базы данных. Он не регламентируется стандартами, и у других регистраторов может быть другим.

Для российского реестра доменов значения полей ответа таково:

- domain: запрашиваемое доменное имя;
- type: тип домена (GEOGRAPHICAL – географический, GENERIC – общего назначения, CORPORATE – все прочие);
- descr: комментарий;
- nserver: DNS-сервера, держащие записи об этом домене;
- state: состояние домена;
- org: имя владельца (для юридических лиц);
- person: имя владельца (для физических лиц);
- nic-hdl: идентификатор владельца в БД регистратора;
- phone: номер телефона владельца;
- fax-no: номер факса владельца;
- e-mail: адрес электронной почты владельца;
- p_addr: почтовый адрес владельца;
- registrar: идентификатор регистратора, зарегистрировавшего этот домен;
- created: дата первичной регистрации;
- paid-till: дата окончания действия регистрации;
- changed: дата последнего изменения записи;
- source: отвечающий whois-сервер.

Проведем еще один опыт по установлению владельца домена. Запросим, например, кто владеет доменом «fsb.ru»:

```
$>whois -c ru fsb.ru
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

domain:      FSB.RU
type:        CORPORATE
nserver:     ns1.fsb.ru. 213.24.76.2
nserver:     ns2.fsb.ru. 194.226.94.138
state:       REGISTERED, DELEGATED
org:         Federal Security Service of Russian Federation
phone:       +7 095 9149084
fax-no:      +7 095 9149084
e-mail:      admin@fsb.ru
registrar:   RTCOMM-REG-RIPN
created:     1998.07.06
paid-till:   2007.08.01
source:      TC-RIPN

Last updated on 2006.12.16 14:36:46 MSK/MSD
```

В качестве регистратора выступает организация, обозначенная идентификатором «RTCOMM-REG-RIPN». Попробуем узнать об этом регистраторе больше. Для этого запросим тот же whois-сервер (ведь все российские регистраторы тоже должны быть зарегистрированы):

```
$>whois -c ru RTCOMM-REG-RIPN
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

nic-hdl:     RTCOMM-REG-RIPN
org:         RTCOMM.RU Open Joint Stock Company
phone:       +7 095 980-01-70
fax-no:      +7 095 980-01-71
e-mail:      osp@rtcomm.ru
www:         www.rtcomm.ru
whois:       whois.rtcomm.ru
source:      TC-RIPN

Last updated on 2006.12.16 14:51:13 MSK/MSD
```

В ответе присутствует указание на собственный whois-сервер регистратора. Как указывалось выше, база данных каждого регистратора является подмножеством общей базы данных и не может ей противоречить. Однако whois-сервер конкретного регистратора может быть настроен иначе и выдаст нам более подробную информацию. Сделаем запрос к whois-серверу регистратора. Для этого используем в команде ключ «-h», после которого стоит имя whois-сервера.

```
$>whois -h whois.rtcomm.ru fsb.ru

domain:      FSB.RU
type:        CORPORATE
descr:       Corporate domain for Federal Security Service
nserver:     ns1.fsb.ru. 213.24.76.2
nserver:     ns2.fsb.ru. 194.226.94.138
state:       REGISTERED, DELEGATED
nic-hdl:     ORG_44-ORG-RTCOMM
org:         Federal Security Service of Russian Federation
p_addr:      103045, Москва
p_addr:      Лубянский проезд, 3/6,
p_addr:      Федеральная Служба Безопасности РФ
p_addr:      Дмитрий Левыкин
p_addr:      Голушко Александр
phone:       +7 095 9149084
fax_no:      +7 095 9149084
e-mail:      admin@fsb.ru
reg-till:    01-08-2007
```



```
created:     06-07-1998
changed:     09-08-2006
registrar:   RTCOMM-REG-RIPN

% Queries frequency limited by 60 per minute.
```

Здесь информации чуть больше. Однако возможности whois себя исчерпали. Для дальнейшей информации следует контактировать с регистратором.

Достоверность данных регистратора

Следует помнить, что данные о владельце домена заносит в базу регистратор. Как для домена RU, так и для других доменов установлен порядок занесения и изменения записей. Разумеется, присутствуют требования об актуальности и достоверности данных. Однако регистраторы не всегда имеют возможности проводить проверку сообщенных им данных. И не всегда вовремя обновляют устаревшие.

Какие же данные о владельце домена можно считать достоверными?

Те, от которых зависит его право распоряжаться доменным именем.

Согласно условиям типового договора большинства регистраторов, указание недостоверных данных о владельце доменного имени может повлечь отмену регистрации. Невозможность связаться по указанным контактным данным также может привести к потере права на доменное имя. Многие регистраторы не позволяют передавать доменные имена иному лицу, пока прежний владелец не представит соответствующие документы. Следовательно, указание неверных контактных данных (телефона, почтового адреса, адреса электронной почты) с немалой вероятностью приводит к потере доменного имени. Указание неверного имени (названия) владельца приводит к тому, что домен нельзя будет передать другому владельцу (продать).

Отсюда можно сделать вывод о том, какие из указанных данных о владельце более достоверны, а какие – менее.

Анонимизация владельцев

Ситуация с регистрацией доменов меняется. В России вступил в силу Федеральный закон «О персональных данных», согласно которому физическое лицо вправе потребовать убрать свои данные из общедоступного источника, каковым является whois-сервис регистратора. ICANN также планирует в ближайшее время внести поправки в правила регистрации доменов, предусматривающие квазианонимность. Владелец сможет указать вместо своих данных контактную информацию третьего лица, например, адвоката или интернет-провайдера, через которых теоретически можно будет выйти на реального владельца.

Тем не менее реальные данные владельца доменного имени должны храниться у регистратора. Для целей уголовного расследования их можно получить, опираясь на закон «О милиции». Для гражданских дел истцам, видимо, придется назначать ответчиком регистратора, затем в ходе судебного разбирательства получать от него персональные данные истинного владельца и затем менять ответчика.

Документирование

Немного сложнее обстоит дело с документированием принадлежности домена.

Как для уголовного, так и для гражданского процесса необходимо доказать, что такое-то доменное имя принадлежит такому-то лицу.

На практике применяются следующие методы (упорядочены от наименее к наиболее предпочтительному):

- Оформить получение справки от whois-сервера рапортом оперуполномоченного. Совсем не безупречный способ. Годится только если обвиняемый (ответчик) не намерен отрицать принадлежность доменного имени.
- Заверить у нотариуса содержимое веб-страницы, представляющей собой веб-интерфейс к команде whois, например, такой, как изображена на последней иллюстрации. Применяется для гражданских дел. Далеко не все нотариусы соглашаются заверять содержимое веб-страниц. Но уж если такого нотариуса удалось найти, то нотариальное заверение производит на суд положительное впечатление. Но для специалиста такой способ – почти профанация, ведь нотариус не видит, к какой именно базе данных подключен веб-интерфейс. Следовательно, его заверение – не более чем заверение надписи на заборе, сделанной неизвестно кем неизвестно для каких целей.
- Получить официальный ответ оператора связи (провайдера), который имел отношение к обслуживанию этого доменного имени, например, поддерживал для него DNS-сервер или веб-сайт. Вместо письма провайдера можно взять показания у соответствующего технического сотрудника этого провайдера.
- Получить показания свидетелей. Например, о том, что интересующее нас лицо совершало определенные действия с доменным именем, доступные только его владельцу.
- Доказать факт оплаты соответствующим лицом услуг по регистрации или продлению домена. Хотя оплачивать можно и чужой домен, но тем не менее это хорошее косвенное доказательство.
- Назначить компьютерно-техническую экспертизу, в ходе которой эксперт запросит нужный whois-сервер и о результатах напишет в своем заключении. Способ несложный, но далеко не безупречный. Сомнительна сама возможность проведения компьютерно-технической экспертизы, когда объект исследования (whois-сервер, база данных регистратора) находится не в распоряжении эксперта, а неизвестно где, на другом конце мира.

- Обнаружить в ходе экспертизы на компьютере соответствующего лица свидетельства соединения и успешной авторизации на интерфейсе регистратора доменов. Практически все регистраторы предоставляют владельцам доменных имен возможность удаленно управлять своими доменами через веб-интерфейс на веб-сайте регистратора. На последующей иллюстрации приводится одна из страниц такого веб-интерфейса регистратора АНО «РСИЦ» (товарный знак «РУ-Центр»). Сам факт успешного доступа к этой странице говорит о прохождении авторизации. Значит, лицо, на компьютере которого обнаружена такая веб-страница, знало верный пароль. А это, скорее всего, означает, что оно и было владельцем домена.
- Получить справку о регистрации доменного имени у соответствующего регистратора или в техническом центре РОСНИИРОС, который поддерживает единую базу данных регистраторов зон RU и SU. Очень хороший способ, но годится только для тех случаев, когда регистратор находится в России, в крайнем случае, в Белоруссии или на Украине. У иностранного регистратора получить такую справку труднее, придется задействовать Интерпол.

Клиентский веб-интерфейс регистратора доменных имен. Обнаружение подобной страницы на диске пользователя свидетельствует о наличии у него договора с регистратором

Принадлежность адреса электронной почты

Сообщения электронной почты фигурируют во многих уголовных и гражданских делах. В некоторых они даже являются центральным доказательством. При помощи электронной почты заключаются сделки, происходит сговор о совершении преступления, совершается вымогательство, передаются существенные для дела сведения. Во всех подобных случаях встает вопрос: кому принадлежит или кем используется тот или иной адрес электронной почты.

Почтовый ящик

В большинстве случаев адрес электронной почты однозначно связан с почтовым ящиком. И все письма, адресованные на этот адрес, попадают в этот ящик, откуда потом пользователь может их забрать.

Однако есть исключения:

- групповые или коллективные адреса, которые представляют собой адрес списка рассылки*; все поступающие на этот адрес письма рассылаются определенной группе адресатов; таковыми часто бывают ролевые адреса, например, `info@company.ru` или `noc@provider.net`;
- технические адреса, за которыми не стоит ни пользователь, ни почтовый ящик; все поступающие на такой адрес письма обрабатываются программой; например, иногда в качестве обратного адреса указывается нечто вроде `noreply@domain.com` — все, что поступает на такой адрес, отправляется почтовым сервером на устройство `/dev/null`;
- адреса для пересылки (forward) сообщений; все поступающие на такой адрес сообщения не складываются в почтовый ящик, а перенаправляются на другой, заранее заданный адрес.

Передача сообщений

В сообщении электронной почты адрес может быть указан в следующих полях. Адрес получателя — в полях «`To`», «`Cc`» и «`Bcc`». Адрес отправителя — в полях «`From`», «`Reply-to`» и «`Return-path`». Парадокс в том, что все эти поля могут не содержать истинного адреса. Все шесть адресов могут быть подложными, но, несмотря на это, сообщение дойдет по назначению. Чтобы пояснить, как такое может быть, рассмотрим процесс передачи сообщения электронной почты по протоколу SMTP.

Ниже приводится образец трафика (снят командой «`tcpdump -i rl0 -s 1024 -n -xX 'tcp and port 25'`»), в котором зафиксирован процесс передачи одного сообщения.

```
21:27:09.265031 IP 190.49.202.78.33594 > 80.94.84.25.25: S
3705705427:3705705427(0) win 64240 <mss 1452,nop,nop,sackOK>
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
```



```
        0x0010:  0030 50d0 4000 6906 9400 be31 ca4e 505e  .0P.@.i....1.NP^
        0x0020:  5419 833a 0019 dce0 93d3 0000 0000 7002  T..:..........p.
        0x0030:  faf0 6737 0000 0204 05ac 0101 0402        ..g7..........

21:27:09.265117 IP 80.94.84.25.25 > 190.49.202.78.33594: S
440205854:440205854(0) ack 3705705428 win 65535 <mss 1460,nop,nop,sackOK>
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  0030 dab6 4000 4006 331a 505e 5419 be31  .0..@.@.3.P^T..1
        0x0020:  ca4e 0019 833a 1a3d 021e dce0 93d4 7012  .N...:.=......p.
        0x0030:  ffff 45b4 0000 0204 05b4 0101 0402        ..E...........

21:27:09.549685 IP 190.49.202.78.33594 > 80.94.84.25.25: . ack 1 win 65340
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  0028 50d9 4000 6906 93ff be31 ca4e 505e  .(P.@.i....1.NP^
        0x0020:  5419 833a 0019 dce0 93d4 1a3d 021f 5010  T..:.......=..P.
        0x0030:  ff3c 733b 0000 0000 0000 0000             .<s;........

21:27:10.177674 IP 80.94.84.25.25 > 190.49.202.78.33594: P 1:86(85) ack 1
win 65535
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  007d dac7 4000 4006 32bc 505e 5419 be31  .}..@.@.2.P^T..1
        0x0020:  ca4e 0019 833a 1a3d 021f dce0 93d4 5018  .N...:.=......P.
        0x0030:  ffff b6b3 0000 3232 3020 6169 6873 2e66  ......220.aihs.f
        0x0040:  6e6e 2e72 7520 4553 4d54 5020 5365 6e64  nn.ru.ESMTP.Send
        0x0050:  6d61 696c 2038 2e31 332e 332f 382e 3133  mail.8.13.3/8.13
        0x0060:  2e33 3b20 5375 6e2c 2031 3420 4a61 6e20  .3;.Sun,.14.Jan.
        0x0070:  3230 3037 2032 313a 3237 3a31 3020 2b30  2007.21:27:10.+0
        0x0080:  3130 3020 2843 4554 290d 0a               100.(CET)..
5
21:27:10.465809 IP 190.49.202.78.33594 > 80.94.84.25.25: P 1:35(34) ack 86
win 65255
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  004a 50e9 4000 6906 93cd be31 ca4e 505e  .JP.@.i....1.NP^
        0x0020:  5419 833a 0019 dce0 93d4 1a3d 0274 5018  T..:.......=.tP.
        0x0030:  fee7 895b 0000 6568 6c6f 2031 3930 2d34  ...[..ehlo.190-4
        0x0040:  392d 3230 322d 3738 2e73 7065 6564 792e  9-202-78.speedy.
        0x0050:  636f 6d2e 6172 0d0a                        com.ar..
6
21:27:10.466320 IP 80.94.84.25.25 > 190.49.202.78.33594: P 86:299(213) ack
35 win 65535
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  00fd dacf 4000 4006 3234 505e 5419 be31  ....@.@.24P^T..1
        0x0020:  ca4e 0019 833a 1a3d 0274 dce0 93f6 5018  .N...:.=.t....P.
        0x0030:  ffff dcd0 0000 3235 302d 6169 6873 2e66  ......250-aihs.f
        0x0040:  6e6e 2e72 7520 4865 6c6c 6f20 3139 302d  nn.ru.Hello.190-
        0x0050:  3439 2d32 3032 2d37 382e 7370 6565 6479  49-202-78.speedy
        0x0060:  2e63 6f6d 2e61 7220 5b31 3930 2e34 392e  .com.ar.[190.49.
        0x0070:  3230 322e 3738 5d20 286d 6179 2062 6520  202.78].(may.be.
        0x0080:  666f 7267 6564 292c 2070 6c65 6173 6564  forged),.pleased
        0x0090:  2074 6f20 6d65 6574 2079 6f75 0d0a 3235  .to.meet.you..25
        0x00a0:  302d 454e 4841 4e43 4544 5354 4154 5553  0-ENHANCEDSTATUS
        0x00b0:  434f 4445 530d 0a32 3530 2d50 4950 454c  CODES..250-PIPEL
        0x00c0:  494e 494e 470d 0a32 3530 2d38 4249 544d  INING..250-8BITM
```

```
        0x00d0:  494d 450d 0a32 3530 2d53 495a 450d 0a32  IME..250-SIZE..2
        0x00e0:  3530 2d44 534e 0d0a 3235 302d 4554 524e  50-DSN..250-ETRN
        0x00f0:  0d0a 3235 302d 4445 4c49 5645 5242 590d  ..250-DELIVERBY.
        0x0100:  0a32 3530 2048 454c 500d 0a               .250.HELP..
7
21:27:10.754272 IP 190.49.202.78.33594 > 80.94.84.25.25: P 35:68(33) ack 299
win 65042
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  0049 50f0 4000 6906 93c7 be31 ca4e 505e  .IP.@.i....1.NP^
        0x0020:  5419 833a 0019 dce0 93f6 1a3d 0349 5018  T..:.......=.IP.
        0x0030:  fe12 8283 0000 4d41 494c 2046 524f 4d3a  ......MAIL.FROM:
        0x0040:  203c 6164 616d 4073 6263 676c 6f62 616c  .<adam@sbcglobal
        0x0050:  2e6e 6574 3e0d 0a                         .net>..
8
21:27:10.764846 IP 80.94.84.25.25 > 190.49.202.78.33594: P 299:344(45) ack
68 win 65535
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  0055 dad6 4000 4006 32d5 505e 5419 be31  .U..@.@.2.P^T..1
        0x0020:  ca4e 0019 833a 1a3d 0349 dce0 9417 5018  .N...:.=.I....P.
        0x0030:  ffff 5f8d 0000 3235 3020 322e 312e 3020  .._...250.2.1.0.
        0x0040:  3c61 6461 6d40 7362 6367 6c6f 6261 6c2e  <adam@sbcglobal.
        0x0050:  6e65 743e 2e2e 2e20 5365 6e64 6572 206f  net>....Sender.o
        0x0060:  6b0d 0a                                    k..
9
21:27:11.052039 IP 190.49.202.78.33594 > 80.94.84.25.25: P 68:93(25) ack 344
win 64997
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  0041 50f7 4000 6906 93c8 be31 ca4e 505e  .AP.@.i....1.NP^
        0x0020:  5419 833a 0019 dce0 9417 1a3d 0376 5018  T..:.......=.vP.
        0x0030:  fde5 753f 0000 5243 5054 2054 4f3a 203c  ..u?..RCPT.TO:.<
        0x0040:  6162 7573 6540 666e 6e2e 7275 3e0d 0a    abuse@fnn.ru>..
10
21:27:11.062441 IP 80.94.84.25.25 > 190.49.202.78.33594: P 344:386(42) ack
93 win 65535
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  0052 dae1 4000 4006 32cd 505e 5419 be31  .R..@.@.2.P^T..1
        0x0020:  ca4e 0019 833a 1a3d 0376 dce0 9430 5018  .N...:.=.v...0P.
        0x0030:  ffff 3875 0000 3235 3020 322e 312e 3520  ..8u..250.2.1.5.
        0x0040:  3c61 6275 7365 4066 6e6e 2e72 753e 2e2e  <abuse@fnn.ru>..
        0x0050:  2e20 5265 6369 7069 656e 7420 6f6b 0d0a  ..Recipient.ok..
11
21:27:11.408007 IP 190.49.202.78.33594 > 80.94.84.25.25: P 93:99(6) ack 386
win 64955
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  002e 50fe 4000 6906 93d4 be31 ca4e 505e  ..P.@.i....1.NP^
        0x0020:  5419 833a 0019 dce0 9430 1a3d 03a0 5018  T..:.....0.=..P.
        0x0030:  fdbb cd44 0000 4441 5441 0d0a             ...D..DATA..
12
21:27:11.408641 IP 80.94.84.25.25 > 190.49.202.78.33594: P 386:436(50) ack
99 win 65535
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  005a dae8 4000 4006 32be 505e 5419 be31  .Z..@.@.2.P^T..1
        0x0020:  ca4e 0019 833a 1a3d 03a0 dce0 9436 5018  .N...:.=.....6P.
```



```
        0x0030:  ffff 1c33 0000 3335 3420 456e 7465 7220  ...3..354.Enter.
        0x0040:  6d61 696c 2c20 656e 6420 7769 7468 2022  mail,.end.with."
        0x0050:  2e22 206f 6e20 6120 6c69 6e65 2062 7920  .».on.a.line.by.
        0x0060:  6974 7365 6c66 0d0a                        itself..
13
21:27:11.745391 IP 190.49.202.78.33594 > 80.94.84.25.25: . 99:1551(1452) ack
436 win 64905
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  05d4 5107 4000 6906 8e25 be31 ca4e 505e  ..Q.@.i..%.1.NP^
        0x0020:  5419 833a 0019 dce0 9436 1a3d 03d2 5010  T..:.....6.=..P.
        0x0030:  fd89 7b52 0000 4d65 7373 6167 652d 4944  ..{R..Message-ID
        0x0040:  3a20 3c30 3030 3030 3163 3733 3831 6124  :.<000001c7381a$
        0x0050:  3661 3739 3762 3830 2434 6563 6133 3162  6a797b80$4eca31b
        0x0060:  6540 4752 4146 4943 4f53 3e0a 4672 6f6d  e@GRAFICOS>.From
        0x0070:  3a20 224a 6f68 6e22 203c 6164 616d 4073  :."John».<adam@s
        0x0080:  6263 676c 6f62 616c 2e6e 6574 3e0a 546f  bcglobal.net>.To
        0x0090:  3a20 3c61 6275 7365 4066 6e6e 2e72 753e  :.<abuse@fnn.ru>
        0x00a0:  0a53 7562 6a65 6374 3a20 4265 7374 2055  .Subject:.Best.U
        0x00b0:  5320 6472 7567 732e 0a44 6174 653a 2053  S.drugs..Date:.S
        0x00c0:  756e 2c20 3134 204a 616e 2032 3030 3720  un,.14.Jan.2007.
        0x00d0:  3137 3a32 373a 3331 202b 3031 3030 0a4d  17:27:31.+0100.M
        0x00e0:  494d 452d 5665 7273 696f 6e3a 2031 2e30  IME-Version:.1.0
        0x00f0:  0a43 6f6e 7465 6e74 2d54 7970 653a 206d  .Content-Type:.m
        0x0100:  756c 7469 7061 7274 2f72 656c 6174 6564  ultipart/related
        0x0110:  3b0a 0974 7970 653d 226d 756c 7469 7061  ;..type="multipa
        0x0120:  7274 2f61 6c74 6572 6e61 7469 7665 223b  rt/alternative";
        0x0130:  0a09 626f 756e 6461 7279 3d22 2d2d 2d2d  ..boundary="----
        0x0140:  2d2d 2d2d 2d2d 2d2d 6d73 3030 3033 3030  --------ms000300
        0x0150:  3037 3034 3039 3030 3035 3036 3039 3034  0704090005060904
        0x0160:  3039 220a 582d 5072 696f 7269 7479 3a20  09».X-Priority:.
        0x0170:  330a 582d 4d53 4d61 696c 2d50 7269 6f72  3.X-MSMail-Prior
        0x0180:  6974 793a 204e 6f72 6d61 6c0a 582d 4d61  ity:.Normal.X-Ma
        0x0190:  696c 6572 3a20 4d69 6372 6f73 6f66 7420  iler:.Microsoft.
        0x01a0:  4f75 746c 6f6f 6b20 4578 7072 6573 7320  Outlook.Express.
        0x01b0:  362e 3030 2e32 3930 302e 3238 3639 0a58  6.00.2900.2869.X
        0x01c0:  2d4d 696d 654f 4c45 3a20 5072 6f64 7563  -MimeOLE:.Produc
        0x01d0:  6564 2042 7920 4d69 6372 6f73 6f66 7420  ed.By.Microsoft.
        0x01e0:  4d69 6d65 4f4c 4520 5636 2e30 302e 3239  MimeOLE.V6.00.29
        0x01f0:  3030 2e32 3936 320a 0a54 6869 7320 6973  00.2962..This.is
        0x0200:  2061 206d 756c 7469 2d70 6172 7420 6d65  .a.multi-part.me
        0x0210:  7373 6167 6520 696e 204d 494d 4520 666f  ssage.in.MIME.fo
        0x0220:  726d 6174 2e0a 0a2d 2d2d 2d2d 2d2d 2d2d  rmat...---------
        0x0230:  2d2d 2d2d 2d6d 7330 3030 3330 3030 3730  -----ms000300070
        0x0240:  3430 3930 3030 3530 3630 3930 3430 390a  409000506090409.
        0x0250:  436f 6e74 656e 742d 5479 7065 3a20 6d75  Content-Type:.mu
        0x0260:  6c74 6970 6172 742f 616c 7465 726e 6174  ltipart/alternat
        0x0270:  6976 653b 0a09 626f 756e 6461 7279 3d22  ive;..boundary="
        0x0280:  2d2d 2d2d 2d2d 2d2d 2d2d 2d2d 6d73 3034  ------------ms04
        0x0290:  3035 3036 3031 3030 3035 3032 3037 3030  0506010005020700
        0x02a0:  3035 3036 3031 220a 0a0a 2d2d 2d2d 2d2d  050601»...------
        0x02b0:  2d2d 2d2d 2d2d 2d2d 6d73 3034 3035 3036  --------ms040506
        0x02c0:  3031 3030 3035 3032 3037 3030 3035 3036  0100050207000506
        0x02d0:  3031 0a43 6f6e 7465 6e74 2d54 7970 653a  01.Content-Type:
```

```
        0x02e0:  2074 6578 742f 6874 6d6c 3b0a 0963 6861  .text/html;..cha
        0x02f0:  7273 6574 3d22 6973 6f2d 3838 3539 2d31  rset="iso-8859-1
        0x0300:  220a 436f 6e74 656e 742d 5472 616e 7366  «.Content-Transf
        0x0310:  6572 2d45 6e63 6f64 696e 673a 2071 756f  er-Encoding:.quo
        0x0320:  7465 642d 7072 696e 7461 626c 650a 0a3c  ted-printable..<
        0x0330:  2144 4f43 5459 5045 2048 544d 4c20 5055  !DOCTYPE.HTML.PU
        0x0340:  424c 4943 2022 2d2f 2f57 3343 2f2f 4454  BLIC."-//W3C//DT
        0x0350:  4420 4854 4d4c 2034 2e30 2054 7261 6e73  D.HTML.4.0.Trans
        0x0360:  6974 696f 6e61 6c2f 2f45 4e22 3e0a 3c48  itional//EN">.<H
        0x0370:  544d 4c3e 3c48 4541 443e 0a3c 4d45 5441  TML><HEAD>.<META
        0x0380:  2068 7474 702d 6571 7569 763d 3344 436f  .http-equiv=3DCo
        0x0390:  6e74 656e 742d 5479 7065 2063 6f6e 7465  ntent-Type.conte
        0x03a0:  6e74 3d33 4422 7465 7874 2f68 746d 6c3b  nt=3D"text/html;
        0x03b0:  2063 6861 7273 6574 3d33 4469 736f 2d38  .charset=3Diso-8
        0x03c0:  3835 392d 3122 3e0a 3c4d 4554 4120 636f  859-1">.<META.co
        0x03d0:  6e74 656e 743d 3344 224d 5348 544d 4c20  ntent=3D"MSHTML.
        0x03e0:  362e 3030 2e32 3930 302e 3239 3935 2220  6.00.2900.2995».
        0x03f0:  6e61 6d65 3d33 4447 454e 4552 4154 4f52  name=3DGENERATOR
14
21:27:11.750983 IP 190.49.202.78.33594 > 80.94.84.25.25: P 1551:1635(84) ack
436 win 64905
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  007c 5108 4000 6906 937c be31 ca4e 505e  .|Q.@.i..|.1.NP^
        0x0020:  5419 833a 0019 dce0 99e2 1a3d 03d2 5018  T..:.......=..P.
        0x0030:  fd89 b6e2 0000 3034 3033 3036 3035 3034  ......0403060504
        0x0040:  3035 3030 3037 3032 3031 3032 3031 404a  05000702010201@J
        0x0050:  6f68 6e3e 0a0a 0a0a 2d2d 2d2d 2d2d 2d2d  ohn>....--------
        0x0060:  2d2d 2d2d 2d2d 6d73 3030 3033 3030 3037  ------ms00030007
        0x0070:  3034 3039 3030 3035 3036 3039 3034 3039  0409000506090409
        0x0080:  2d2d 0a0a 0a0a 0a0a                       --........
15
21:27:11.751073 IP 80.94.84.25.25 > 190.49.202.78.33594: . ack 1635 win
65535
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  0028 daeb 4000 4006 32ed 505e 5419 be31  .(..@.@.2.P^T..1
        0x0020:  ca4e 0019 833a 1a3d 03d2 dce0 9a36 5010  .N...:.=.....6P.
        0x0030:  ffff 6a63 0000 0000 0000 0000             ..jc........
16
21:27:12.035765 IP 190.49.202.78.33594 > 80.94.84.25.25: P 1635:1640(5) ack
436 win 64905
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  002d 5115 4000 6906 93be be31 ca4e 505e  .-Q.@.i....1.NP^
        0x0020:  5419 833a 0019 dce0 9a36 1a3d 03d2 5018  T..:.....6.=..P.
        0x0030:  fd89 27b5 0000 0d0a 2e0d 0a00             ..'.........
17
21:27:12.042413 IP 80.94.84.25.25 > 190.49.202.78.33594: P 436:492(56) ack
1640 win 65535
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  0060 daf4 4000 4006 32ac 505e 5419 be31  .`..@.@.2.P^T..1
        0x0020:  ca4e 0019 833a 1a3d 03d2 dce0 9a3b 5018  .N...:.=.....;P.
        0x0030:  ffff d11e 0000 3235 3020 322e 302e 3020  ......250.2.0.0.
        0x0040:  6c30 454b 5241 4647 3033 3434 3438 204d  l0EKRAFG034448.M
        0x0050:  6573 7361 6765 2061 6363 6570 7465 6420  essage.accepted.
```



```
        0x0060:  666f 7220 6465 6c69 7665 7279 0d0a       for.delivery..
18
21:27:12.327003 IP 190.49.202.78.33594 > 80.94.84.25.25: P 1640:1646(6) ack
492 win 64849
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  002e 511d 4000 6906 93b5 be31 ca4e 505e  ..Q.@.i....1.NP^
        0x0020:  5419 833a 0019 dce0 9a3b 1a3d 040a 5018  T..:.....;.=..P.
        0x0030:  fd51 84d2 0000 7175 6974 0d0a             .Q....quit..
19
21:27:12.327578 IP 80.94.84.25.25 > 190.49.202.78.33594: P 492:534(42) ack
1646 win 65535
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  0052 db09 4000 4006 32a5 505e 5419 be31  .R..@.@.2.P^T..1
        0x0020:  ca4e 0019 833a 1a3d 040a dce0 9a41 5018  .N...:.=.....AP.
        0x0030:  ffff 9e49 0000 3232 3120 322e 302e 3020  ...I..221.2.0.0.
        0x0040:  6169 6873 2e66 6e6e 2e72 7520 636c 6f73  aihs.fnn.ru.clos
        0x0050:  696e 6720 636f 6e6e 6563 7469 6f6e 0d0a  ing.connection..

21:27:12.328061 IP 80.94.84.25.25 > 190.49.202.78.33594: F 534:534(0) ack
1646 win 65535
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  0028 db0a 4000 4006 32ce 505e 5419 be31  .(..@.@.2.P^T..1
        0x0020:  ca4e 0019 833a 1a3d 0434 dce0 9a41 5011  .N...:.=.4...AP.
        0x0030:  ffff 69f5 0000 0000 0000 0000             ..i.........

21:27:12.613806 IP 190.49.202.78.33594 > 80.94.84.25.25: F 1646:1646(0) ack
534 win 64807
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  0028 5126 4000 6906 93b2 be31 ca4e 505e  .(Q&@.i....1.NP^
        0x0020:  5419 833a 0019 dce0 9a41 1a3d 0434 5011  T..:.....A.=.4P.
        0x0030:  fd27 6ccd 0000 0000 0000 0000             .'l.........

21:27:12.613974 IP 80.94.84.25.25 > 190.49.202.78.33594: F 534:534(0) ack
1647 win 65535
        0x0000:  0013 7f8d f11a 0050 22ee 207d 0800 4500  .......P»..}..E.
        0x0010:  0028 db0e 4000 4006 32ca 505e 5419 be31  .(..@.@.2.P^T..1
        0x0020:  ca4e 0019 833a 1a3d 0434 dce0 9a42 5011  .N...:.=.4...BP.
        0x0030:  ffff 69f4 0000 0000 0000 0000             ..i.........

21:27:12.617338 IP 190.49.202.78.33594 > 80.94.84.25.25: . ack 535 win 64807
        0x0000:  0050 22ee 207d 0013 7f8d f11a 0800 4500  .P»..}........E.
        0x0010:  0028 5127 4000 6906 93b1 be31 ca4e 505e  .(Q'@.i....1.NP^
        0x0020:  5419 833a 0019 dce0 9a42 1a3d 0435 5010  T..:.....B.=.5P.
        0x0030:  fd27 6ccc 0000 0000 0000 0000             .'l.........
```

После установления соединения (первые три пакета) принимающий сервер дает код 220 и некоторые данные о себе (4-й пакет). Передающий сервер дает команду «**EHLO**» и свой идентификатор (5-й пакет). Принимающий сервер дает код 250 и некоторые свои параметры (6-й пакет). Передающий сервер дает команду «**MAIL FROM**» (7-й пакет), затем команду «**RCPT TO**» (9-й пакет). Принимающий подтверждает допустимость этих команд

кодом 250 (8-й и 10-й пакеты). Затем передающий сервер дает команду «DATA» (11-й пакет), а принимающий подтверждает кодом 354 готовность принимать текст письма (12-й пакет). Передающий сервер отправляет текст сообщения, включая все заголовки (пакеты 13, 14 и 16). Принимающий подтверждает прием кодом 250 (17-й пакет). Затем передающий дает команду «QUIT» (18-й пакет), на что получает код 221 (19-й пакет). Остальные пакеты завершают TCP-соединение. Так работает протокол SMTP.

Передающий MTA	**Принимающий MTA**
	220
HELO или EHLO	
	250
MAIL FROM: <адрес>	
	250
RCPT TO: <адрес>	
	250
DATA	
	354
текст сообщения	
.	
	250
QUIT	
	221

Достоверность

Как видно, все заголовки сообщения («From», «To» и другие) передаются в тексте письма, они могут не анализироваться принимающей стороной. Куда именно следует доставить сообщение, принимающий сервер узнает из команды «RCPT TO», адрес в которой не обязан совпадать с адресом в заголовке «To».

Наличие какого-либо адреса в поле «From» или «Reply-to» означает лишь то, что отправитель счел нужным вписать туда этот адрес. Каких-либо достоверных выводов об источнике или отправителе письма при этом сделать невозможно. Источник и отправитель могут быть вычислены из анализа заголовков «Received» и соответствующих логов серверов электронной почты, как это описано в предыдущей главе.

Но если подтверждено, что адрес действующий, то есть некое лицо получает отправленные на него письма, то можно браться за установление владельца этого адреса.

Установление

Для начала следует установить почтовый ящик, с которым связан адрес. Затем выяснить, кто пользуется этим почтовым ящиком. Так будет установлен владелец адреса.

Для установки места расположения почтового ящика исследователь устанавливает первичный MX домена. Во многих случаях ящик находится на этом же сервере. В других случаях сервер пересылает почту на иной сервер, указанный в его настройках. В обоих случаях требуется узнать эти настройки, чтобы определить местоположение почтового ящика. Для этого потребуется содействие провайдера, обслуживающего сервер. Расположение почтового ящика документируется протоколом осмотра нужного сервера (серверов) или заключением эксперта. В крайнем случае, можно ограничиться получением письменного ответа провайдера на соответствующий запрос, но этот способ доказательства нельзя назвать безупречным.

Доказательствами факта использования почтового ящика определенным лицом могут служить:

- наличие на компьютере этого лица настроек для доступа к этому ящику (включая пароль);
- наличие на компьютере этого лица полученных сообщений электронной почты со служебными заголовками, свидетельствующими о прохождении сообщений через этот почтовый ящик;
- наличие на сервере, где расположен ящик, логов об успешном соединении и аутентификации пользователя данного почтового ящика;
- наличие у других абонентов сообщений от этого лица, написанных в ответ на сообщения, отправленные на этот почтовый ящик (в ответе часто цитируется исходное сообщение, а также среди служебных заголовков присутствует заголовок со ссылками на предыдущие сообщения).

Примеры

Три примера на тему установления владельца адреса электронной почты и доказывания этого факта.

В ходе расследования преступления было установлено, что обнаруженная на компьютере потерпевшего вредоносная программа пытается отослать некоторые данные по электронной почте. Эксперт запустил эту программу на своем компьютере, маршрутизировал весь исходящий трафик с него на другой компьютер, на котором запустил эмулятор внешнего SMTP-сервера. В результате эксперимента обнаружилось, что неизвестная вредоносная программа отсылает по электронной почте письмо на адрес user0001@pnzhost.ru. В этом письме содержалась конфиденциальная информация с компьютера потерпевшего.

Соответствующая DNS-запись (запись типа MX) указывает, что сервер входящей электронной почты для домена pnzhost.ru имеет IP-адрес 133.245.254.110. Этот IP-адрес, согласно данным регистратора, используется провайдером* «Заречный телеком» из города Пензы. Все эти данные были установлены привлеченным специалистом в ходе ОРМ «иссле-

дование предметов и документов». По данным из whois, можно было предположить, что указанный IP-адрес используется не самим провайдером для собственных нужд, а сервером одного из клиентов этого провайдера.

Сделан запрос в ЗАО «Заречный телеком». Официальный ответ пришел по почте лишь через три недели, но оперуполномоченный, пользуясь личными контактами с работником провайдера, получил быстрый неофициальный ответ, что упомянутый IP-адрес `133.245.254.110` действительно используется сервером одного из клиентов по фамилии Семенов; на этом сервере оказываются услуги хостинга*. Кроме того, присутствует услуга бесплатного хостинга: каждый желающий может получить место для веб-сайта и ящик электронной почты. Предположительно, именно такой бесплатный анонимный ящик и соответствует адресу user0001@pnzhost.ru

Проведен осмотр указанного сервера. В логах обнаружены несколько записей о доступе к почтовому ящику по протоколу POP3 с IP-адресов `220.12.122.3, 220.12.122.16, 220.12.122.55`. Эти адреса относятся к одному пулу, который, как установлено, используется провайдером «МСК-Антен» для оказания услуги коммутируемого доступа.

Далее последовал запрос к этому провайдеру. Очень хорошо, что при осмотре логов сервера были зафиксированы не только адреса, но и точное время каждого обращения, а также погрешность внутренних часов сервера, поскольку IP-адреса оказались динамическими*. По ним был установлен номер телефона абонента.

Итак, доказательствами принадлежности адреса электронной почты явились:

- протокол ОРМ об исследовании документов с указанием на «Заречный телеком», за которым зарегистрирован адрес `133.245.254.110`, являющийся MX для домена электронной почты `pnzhost.ru`;
- ответ от ЗАО «Заречный телеком», подтверждающий использование ими IP-адреса `133.245.254.110` для сервера клиента Семенова;
- протокол выемки документов и изъятый договор с бланк-заказом клиента Семенова;
- показания Семенова, владельца сервера, на котором живет домен электронной почты `pnzhost.ru`;
- протокол осмотра сервера Семенова с фрагментами логов об осуществлении доступа к почтовому аккаунту* `user0001` с IP-адресов из подсети `220.12.122.0`;
- ответ от ЗАО «МСК-Антен» о том, что запрошенные 3 IP-адреса в указанные моменты времени динамически выделялись одному и тому же пользователю с идентификатором «av00387205» и номером телефона 4580445;
- ответ от телефонного узла, что указанный номер закреплен за абонентом Кучеровым, проживающим по адресу: Москва, Правобережная улица, д. 1, кв. 2;

- заключение эксперта по компьютеру, изъятому при обыске в квартире Кучерова по указанному адресу, о том, что с этого компьютера осуществлялся доступ по протоколу POP3 к серверу `133.245.254.110`, а также о том, что для доступа в Интернет использовался логин «av00387205» и 3 IP-адреса из пула провайдера «МСК-Антен».

Конечно же, не все перечисленные доказательства безупречны. Конечно, вместо осмотра логов предпочтительно было бы сделать экспертизу. А кроме ответов на запросы было бы полезно сделать выемку документов у этих операторов связи или хотя бы допросить их технических специалистов. Однако для нашей российской практики и такая цепочка доказательств выглядит достижением. Небезупречная, зато замкнутая.

Во втором примере злоумышленник воспользовался иностранным мейл-сервером.

В ходе расследования дела о вымогательстве было установлено, что потерпевший получил предложение вымогателя по электронной почте. Сообщение пришло с адреса **`vera3456@yahoo.com`** (этот адрес был указан в поле **`From`**). Потерпевший вступил в переписку, пользуясь указанным адресом, и получил несколько ответов на свои письма.

Потерпевший передал на экспертизу свой компьютер, где хранились сообщения, полученные и отправленные им. В одном из сообщений вымогателя в заголовках имелся IP-адрес его домашнего компьютера **`217.225.194.202`** (прочие сообщения он отправлял с использованием анонимизирующего прокси-сервера*).

При получении денег вымогатель был задержан. При обыске у него изъят компьютер. Экспертиза обнаружила на нем фрагменты архива полученных и отправленных сообщений электронной почты, среди которых нашлись и сообщения от потерпевшего, адресованные на **`vera3456@yahoo.com`**, с которого они автоматически перенаправлялись на адрес вымогателя.

Получить информацию от зарубежного оператора связи, поддерживающего почтовый ящик в домене yahoo.com, оказалось невозможно.

Привлеченный судом специалист сопоставил сообщения, найденные экспертами на двух компьютерах (потерпевшего и подсудимого), и сделал вывод, что пользователь второго компьютера действительно получал те сообщения, которые отправлялись пользователем первого компьютера на адрес **`vera3456@yahoo.com`**.

Итак, доказательствами принадлежности адреса электронной почты явились:

- показания потерпевшего об отправлении и получении писем;
- заключение эксперта по компьютеру потерпевшего;
- заключение эксперта по компьютеру подозреваемого;
- заключение специалиста о сопоставлении данных из этих двух экспертиз;

- комплекс доказательств, установивший принадлежность IP-адреса `217.225.194.202` к компьютеру подозреваемого.

Здесь была опущена третья «точка опоры» в лице почтового сервера провайдера. Дело опиралось на совпадение сообщений на компьютерах отправителя и получателя. Возможно, при отсутствии иных доказательств вины двух «опор» и не хватило бы. Но задержание вымогателя при передаче денег не оставляло у следствия и суда никаких сомнений.

Третий пример будет, так сказать, негативным.

При расследовании сбыта номеров банковских карт и поддельных банковских карт было установлено, что подозреваемый осуществлял контакты с покупателями при помощи электронной почты. При этом он использовал адрес `bigbuyer@123card.com` – принимал сообщения на этот адрес и отправлял ответы с него.

Специалист установил, что сервер электронной почты (MX*), соответствующий почтовому домену `123card.com`, имеет IP-адрес `80.12.254.4`, и этот адрес используется провайдером «Condor-Net GmbH» из Германии. Тот же IP-адрес присутствовал в заголовках сообщений, полученных от подозреваемого.

Оперативники посчитали, что позже, когда будет возбуждено уголовное дело, у провайдера можно будет получить сведения о клиенте и логи доступа к аккаунту и связать таким образом адрес `bigbuyer@123card.com` с подозреваемым.

Однако когда дело дошло до получения сведений о клиенте провайдера «Condor-Net GmbH», обнаружилось, что данный клиент воспользовался услугой аренды виртуального сервера. Все настройки такого сервера клиент делает самостоятельно. Все логи, относящиеся к электронной почте, могут лежать только на сервере клиента. Провайдер же не логирует сетевую активность клиентов, кроме учета общего объема трафика. К моменту, когда немецкая полиция провела по поручению российской стороны следственные действия, все содержимое виртуального сервера было уже клиентом (или кем-то другим) вычищено. Никаких логов (если они вообще велись) не осталось.

Договор между провайдером и клиентом заключался через акцепт публичной оферты, размещенной на веб-сайте, а оплата производилась кредитной картой. Указанные клиентом данные оказались вымышленными, а использованная карта – чужой. Таким образом, не было даже доказательств того, что подозреваемый пользовался арендованным сервером `80.12.254.4`.

На компьютере у подозреваемого эксперт не обнаружил следов взаимодействия с сервером `80.12.254.4` или сообщений с адресом `bigbuyer@123card.com`.

Домен `123card.com` был зарегистрирован на имя одного из сообщников подозреваемого, однако этого недостаточно, чтобы доказать использование подозреваемым указанного адреса электронной почты.

В результате из-за невозможности доказать получение и отправку подозреваемым сообщений электронной почты пришлось уголовное дело прекратить.

Кейлогеры

Кейлогерами (keyloggers) называют устройства (программные или аппаратные) для перехвата сигналов с клавиатуры, то есть для записи последовательности нажатых пользователем клавиш.

Большинство паролей набирается с клавиатуры. С нее же вводится большая часть переписки, персональных данных и иной информации, которая может интересовать злоумышленников. Поэтому сбор информации о нажатых клавишах является эффективным способом совершения различных компьютерных преступлений.

Наряду с этим кейлогер может служить инструментом для проведения ОРМ.

Кейлогер можно отнести к устройствам двойного назначения. У него есть ряд легальных применений: отслеживание владельцем случаев несанкционированного использования его собственного компьютера, архивирование информации пользователя на случай ее утраты при сбоях. Тем не менее очевидно, что основным предназначением кейлогеров является скрытное (негласное) получение информации.

Аппаратные кейлогеры

Они выполнены в виде переходника, который вставляется в разрыв клавиатурного кабеля. Бывают аппаратные устройства, которые встроены непосредственно в клавиатуру.

Аппаратные кейлогеры. Вставляются в разрыв между клавиатурой и системным блоком. Не могут быть детектированы программным способом, зато легко обнаруживаются визуально

Современный кейлогер имеет встроенную память на сотни килобайт или несколько мегабайт, собранную информацию хранит в зашифрованном виде. Взаимодействие с «хозяином» обычно строится на том же самом интерфейсе, то есть при помощи клавиатуры, в которую он включен.

Любой желающий может без формальностей приобрести аппаратный кейлогер по цене 150-200 долларов.

Программные кейлогеры

Такие программы доступны как за деньги, так и бесплатно. Как правило, они выполнены по технологиям, используемым в троянских программах, каковыми, по сути, и являются.

Большинство программных кейлогеров будут признаны вредоносными программами, поскольку приспособлены для скрытного внедрения и незаметной для пользователя работы. Однако некоторые из них, имеющие «открытый» режим, добросовестный эксперт вредоносной программой не признает.

Многие программные кейлогеры имеют дополнительные функции – запись движений мыши и снятие скриншотов*.

Интернет-поиск как метод ОРД

Для начала несколько примеров.

Потерпевшим было получено по электронной почте письмо с предложением перевести некую сумму через систему «WebMoney» под угрозой разглашения данных об уязвимости его веб-сервера. Выкуп предлагалось перевести на счет (кошелек) номер `Z18364577`. Пока один оперативник выяснял у сотрудников платежной системы, кем использовался этот счет, другой ввел строку «`Z18364577`» в поисковой системе. Оказалось, что этот номер кошелька уже засвечен в Интернете. Один пользователь жаловался, что перевел на него деньги в оплату за некую услугу, но обещанной услуги не получил. Таким образом нашелся второй потерпевший, в деле появился второй эпизод и дополнительные доказательства.

Поступило заявление о клевете. Неизвестный злоумышленник разместил на веб-форуме информацию, порочащую деловую репутацию потерпевшего. К сожалению, не удалось установить, с какого IP-адреса происходило размещение информации, поскольку злоумышленник воспользовался анонимным прокси-сервером. Тогда оперативник предположил, что преступник мог разместить ту же информацию и на иных интернет-ресурсах. Он ввел характерную фразу из размещенной статьи в поисковую систему и нашел два других веб-форума, на которых, по-видимому, тот же злоумышленник разместил ту же информацию. Во всех случаях он воспользовался анонимизирующим прокси-сервером. Однако на одном из найденных форумов, кроме вышеописанного клеветнического материала, было обнаружено еще несколько постингов (статей), судя по их содержанию, размещенных тем же человеком. Размещенных уже без использования прокси. По ним-то оперативники и вышли на исполнителя.

Подозреваемый в мошенничестве кардер*, задержанный в Москве, был отпущен под подписку о невыезде и немедленно скрылся. Оперуполномоченный для розыска подозреваемого нашел в деле несколько адресов электронной почты, которыми тот пользовался в разное время. Поиск в Интернете по этим адресам среди прочих результатов принес одно объявление о продаже номеров кредитных карт. Объявление было размещено давно и явно неактуально. Однако кроме адреса электронной почты в объявлении был указан для контактов также номер ICQ*. Оперативник предположил, что подозреваемый может до сих пор пользоваться этим номером. Он ввел номер в контакт-лист своего ICQ-клиента и стал ждать, когда абонент «выйдет в эфир», то есть будет обозначен как «online». Через несколько недель это случилось. Подозреваемый стал пользоваться своим номером ICQ почти ежедневно. Оперативник пытался определить IP-адрес, с которого подозреваемый соединяется, но без прямого контакта с ним это оказалось невозможным. Тогда оперуполномоченный вторично обратился к поисковой системе и стал искать, где еще упоминается номер ICQ подозреваемого. И нашел относительно свежее объявление, касающееся организации DoS-атак на сервер. Это дало повод для контакта. Оперативник по ICQ вышел на контакт с подозреваемым и ежедневно общался с ним, пользуясь найденным предлогом. При обмене сообщениями по ICQ есть возможность определить IP собеседника (правда, не во всех случаях). В течение нескольких дней общения в качестве IP подозреваемого детектировался адрес socks-сервера*. Но однажды высветился IP-адрес, похожий на реальный. Он числился за германским провайдером из города Франкфурт-на-Майне. Согласно материалам дела, у подозреваемого в этом городе жил родственник. Дальнейшее было делом техники. Через провайдера установили адрес, и через несколько дней немецкая полиция подозреваемого арестовала. Не прошло и года, как он был экстрадирован в Россию.

Поисковые системы в Интернете стали не только основной «дорогой в сеть» для обычных пользователей, они также широко используются злоумышленниками. При помощи поисковых систем завлекаются жертвы на веб-сайты мошенников. При помощи поисковых систем находятся как сведения об уязвимостях, так и сервера, имеющие эти уязвимости. При помощи поисковых систем маскируется местоположение веб-сайтов. При помощи поисковых систем определяются перспективные слова для киберсквоттинга*. И так далее. В работе специалистов по защите ин-

формации поисковые системы также используются широко. Почему бы не использовать их и в оперативной работе?

Для криминалистики поисковые системы представляют большой интерес, поскольку в них также можно обнаружить следы. Очень многие виды сетевой активности оставляют след в поисковых системах. И этот след не только проще найти, но в ряде случаев он держится в базе данных поисковика дольше, чем в оригинальном расположении.

Например, в ходе одного гражданского дела о нарушении авторских прав истец смог доказать факт размещения ответчиком произведения в сети, хотя ответчик к тому моменту уже успел убрать его с веб-сайта. Но в базе данных двух поисковых систем первоначальная версия сайта ответчика осталась. Заверенные нотариусом распечатки страниц поисковых систем с кэшированным содержимым сайта ответчика признаны судом достаточным доказательством того факта, что в прошлом произведение размещалось в Сети и было общедоступно.

Также поисковик полезен для других задач. Например, для декомпиляции программ. С целью исследования программ для ЭВМ, доступных исследователю только в виде исполняемого (объектного*) кода, можно воспользоваться декомпилятором. Но проблема в том, что восстановленный таким образом исходный текст* малопонятен для человека и не соответствует исходному тексту, из которого был сделан объектный код. Говорят, что операция компиляции исходного текста необратима. Вместо декомпиляции можно провести поиск в Интернете на предмет исходного кода этой же программы [57]. Злоумышленник, скорее всего, не написал свою программу с нуля, а позаимствовал ее целиком или немного модифицировал чужую программу, взяв ее из того же источника – из Сети. Невозможно по исполняемому коду восстановить исходный код* программы на алгоритмическом языке высокого уровня, но возможно доказать, что найденный исходный код соответствует имеющемуся исполняемому коду.

С другой стороны, со стороны поисковой системы тоже можно вести оперативно-розыскную деятельность. Или получать данные в ходе следственных действий. Поисковая система может протоколировать и сохранять все действия пользователя. Объем этой информации относительно невелик, поэтому хранить ее можно без особых затрат на протяжении нескольких лет. Судя по всему, поисковики так и делают.

Когда и какие поисковые запросы отправлял пользователь, по каким из показанных ему ссылок переходил – эти сведения могут быть полезны в ОРД и послужить косвенными доказательствами по уголовному делу.

Поисковая система идентифицирует пользователя по cookie-файлу, а также другим доступным через протокол HTTP параметрам (IP-адрес, версия браузера и ОС, язык, местное время и т.д.).

По некоторым уголовным делам, обнаружив на компьютере подозреваемого cookie от поисковой системы, имеет смысл затребовать протокол действий этого пользователя у администрации поисковика. При этом нужно будет предоставить содержимое cookie и параметры браузера. Разумеется, потребуется судебная санкция.

Заключение к разделу 2

Мы рассмотрели некоторые, наиболее часто употребляемые виды оперативно-розыскных мероприятий по компьютерным преступлениям и методы их проведения.

В подавляющем большинстве случаев для проведения таких мероприятий не требуется специального оборудования или специальных программных средств. Вполне достаточно обычных средств, имеющихся в распоряжении любого оператора связи. Зато специальные знания необходимы всегда.

Автор еще раз хотел бы обратить внимание, что специальные знания требуются не только, чтобы правильно собирать и документировать доказательства. Специальные знания нужны, чтобы знать, где именно эти доказательства искать. Устройство современных ЭВМ и компьютерных сетей настолько сложно, что следы различных действий остаются в самых неожиданных местах. Неожиданных – для обычного пользователя. А для специалиста, глубоко знающего устройство сетей, – вполне очевидных. И чем глубже его знания, тем больше цифровых доказательств он может обнаружить.

3. Следственные действия

Осмотр компьютера

Особенности

Когда следы совершенного преступления и возможные доказательства находятся в цифровой форме (в форме компьютерной информации), их получение, фиксация и документирование представляют определенную сложность.

В отличие от многих иных видов доказательств, компьютерная информация не может восприниматься человеком непосредственно – глазами, ушами, пальцами. Воспринимать ее можно только через посредство технических аппаратных и программных средств. Причем количество и сложность этих технических посредников настолько велики, что связь между исходной информацией и тем, что мы видим не экране, не слишком прямая и далеко не всегда очевидная. А порой эта связь и вовсе условна и зыбка до невозможности (см. главу «Общенаучные методы»).

Следует признать, что осмотр компьютерной информации – это не вполне осмотр (от слова «смотреть»), а скорее инструментальная проверка, требующая определенных знаний об используемых технических средствах, принцип действия которых не всегда очевиден. Вероятность ошибиться и увидеть не то, что есть на самом деле, при этом повышенная, даже при отсутствии целенаправленного воздействия противника.

Высказывалось мнение, что на основании вышеизложенного осмотр компьютерной информации вообще недопустим, а следует всегда проводить экспертизу.

Практика же никак не позволяет принять это утверждение. Провести компьютерно-техническую экспертизу (КТЭ) не всегда возможно даже в тех случаях, когда она точно нужна. Замена экспертизы осмотром позволяет сэкономить очень много времени и сил. Порой перед следователем стоит выбор: или проводить вместо КТЭ осмотр компьютерной информации, или вовсе прекращать дело.

Кроме того, есть и такое соображение. Для проведения КТЭ все равно необходимо изъять носитель информации или скопировать его содержимое. А эти действия по своей сложности и по применению специальных знаний не сильно отличаются от осмотра компьютерной информации на месте. Все равно нужен специалист. Все равно желательны квалифицированные понятые. Все равно действия эксперта сведутся к просмотру и распечатке нужных данных. Так не проще ли произвести эти же действия в порядке осмотра (ст. 176-177 УПК)?

Стандарты

Правила сбора и фиксации цифровых доказательств (то есть компьютерной информации, используемой в качестве доказательства) не закреплены в законе. Нет и ведомственных нормативных актов, закрепляющих такие правила. А потом в суде возникает вопрос: были ли доказательства собраны надлежащим образом, который обеспечивал их достоверность и неизменность? Оценить правильность примененных процедур без специальных знаний невозможно. Когда же существуют официальные или, по крайней мере, общепризнанные правила обращения с цифровыми доказательствами, обосновать достоверность и неизменность значительно проще.

В отношении других видов доказательств, которыми криминалисты занимаются давно, такие правила существуют.

Закрепление стандартов обращения с цифровыми доказательствами в законодательстве невозможно в силу быстрой изменчивости компьютерных систем. Новые устройства, новые носители, новые протоколы, для которых потребны новые процедуры, появляются несколько раз в год. Ежегодно появляются принципиально новые устройства, которые требуют принципиально иного подхода при обнаружении и изъятии цифровых доказательств. Ведомственные методики [85, 86] можно менять достаточно часто. Однако их разработка в нашей стране затруднена отсутствием грамотных технических специалистов в этих ведомствах.

Столкнувшись с необходимостью подобных стандартов, специалисты предложили зафиксировать их на уровне рекомендаций научных или общественных профессиональных организаций. Исполнение таких стандартов, безусловно, снимет ряд возможных вопросов со стороны суда и участников процесса. Автор рекомендует три подобных документа [W28, 7, 11], изданных достаточно авторитетными в области форензики организациями. Изложенный в них опыт учтен при написании разделов 2 и 3 настоящей книги.

Автор предлагает соблюдать при проведении следственных действий требования таких документов и в дальнейшем ссылаться на них для подтверждения «соблюдения общепринятых и признанных ведущими специалистами правил и стандартов».

Лог-файлы, доказательная сила логов

Определение

Лог (компьютерный лог, компьютерный журнал регистрации событий) – это организованная в виде файла, базы данных или массива в оперативной памяти совокупность записей о событиях, зафиксированных какой-либо программой, группой программ, информационной системой. Лог ведется автоматически, без участия человека. Как правило, соблюдается принцип: одно событие – одна запись. Как правило, каждая запись снабжается меткой времени. Обычно записи сохраняются по мере их генерирования, по возможности, независимо от генерирующей их программы, чтобы они оказались доступны для изучения даже в случае сбоя или аварийного завершения программы.

Форма записей может быть произвольной, на усмотрение создателя программы или оператора, производившего ее настройку. Записи лога могут иметь более «гуманитарную» форму, то есть ориентироваться на восприятие человеком. Записи могут быть машинно-ориентированными, то есть предназначаться для легкого восприятия другой программой. Чаще придерживаются промежуточной формы.

Ведение логов может осуществляться само́й генерирующей программой, а может быть передано специализированной (логирующей) программе, такой как «syslogd». Ведение логов (логирование) включает: запись их в соответствующий файл или базу данных, снабжение меткой времени и идентификатором источника, агрегирование (объединение одинаковых или схожих записей), своевременное удаление старых записей и т.д.

Примеры

Ниже автор счел полезным привести образцы некоторых логов, чтобы те читатели, которые редко с ними сталкивались, чувствовали себя более уверенно при изучении дальнейшего материала.

Фрагмент лога сервера электронной почты «sendmail» версии 8.13.3:

```
Dec 14 14:43:12 aihs sm-mta[5156]: kBEDhBbL005156: from=<sonya95wen-
king@barnhallrfc.com>, size=6093, class=0, nrcpts=1,
msgid=<9bd701c71f85$6f70e79a$93c9135a@barnhallrfc.com>, proto=SMTP,
daemon=IPv4, relay=ayc250.internetdsl.tpnet.pl [83.18.106.250]

Dec 14 14:43:16 aihs sm-mta[5157]: kBEDhBbL005156: to=fnn@home.fnn,
delay=00:00:04, xdelay=00:00:04, mailer=esmtp, pri=36347, relay=home.fnn.
[80.94.84.26], dsn=2.0.0, stat=Sent (kBEDhG4D014447 Message accepted for
delivery)

Dec 14 14:44:17 aihs sm-mta[5171]: kBEDiFQH005171:
from=<vt@prostimenya.com>, size=8217, class=0, nrcpts=1,
msgid=<0458524863.20061214073716@prostimenya.com>, bodytype=8BITMIME,
```



```
proto=SMTP, daemon=IPv4, relay=customer.klimatstroy.195.sls-hosting.com
[204.14.1.195]

Dec 14 14:44:17 aihs sm-mta[5172]: kBEDiFQH005171: to=/dev/null,
ctladdr=bit-bucket (26/0), delay=00:00:01, xdelay=00:00:00, mailer=*file*,
pri=38486, dsn=2.0.0, stat=Sent

Dec 14 14:44:39 aihs sm-mta[5173]: kBEDiZU2005173: from=<terri2546zelig@bar-
bary.com>, size=6089, class=0, nrcpts=1,
msgid=<848e01c71f85$0df14333$eb8ddf52@barbary.com>, proto=SMTP, daemon=IPv4,
relay=[59.24.163.104]

Dec 14 14:44:39 aihs sm-mta[5174]: kBEDiZU2005173: to=/dev/null,
ctladdr=bit-bucket (26/0), delay=00:00:03, xdelay=00:00:00, mailer=*file*,
pri=36311, dsn=2.0.0, stat=Sent

Dec 14 14:50:12 aihs sm-mta[5190]: kBEDoAM6005190: from=<yhky@vampismo.com>,
size=8177, class=0, nrcpts=1,
msgid=<9454295755.20061214074311@vampismo.com>, bodytype=8BITMIME,
proto=SMTP, daemon=IPv4, relay=customer.klimatstroy.195.sls-hosting.com
[204.14.1.195]

Dec 14 14:50:12 aihs sm-mta[5191]: kBEDoAM6005190: to=/dev/null,
ctladdr=bit-bucket (26/0), delay=00:00:01, xdelay=00:00:00, mailer=*file*,
pri=38444, dsn=2.0.0, stat=Sent

Dec 14 14:53:42 aihs sm-mta[5192]: kBEDrduu005192:
from=<vvvaldiswwh@gmail.com>, size=8704, class=0, nrcpts=1,
msgid=<67a901c71f88$f5e3e54e$f00600ff@gmail.com>, bodytype=8BITMIME,
proto=ESMTP, daemon=IPv4, relay=msk-m10-st01.rtcomm.ru [213.59.0.34]

Dec 14 14:53:42 aihs sm-mta[5193]: kBEDrduu005192: to=/dev/null,
ctladdr=bit-bucket (26/0), delay=00:00:03, xdelay=00:00:00, mailer=*file*,
pri=38935, dsn=2.0.0, stat=Sent

Dec 14 14:54:17 aihs sm-mta[5194]: kBEDsGgS005194:
from=<ynrripinahov@yahoo.com>, size=8734, class=0, nrcpts=1,
msgid=<7fee01c71f8e$052ada06$eb62a1f3@yahoo.com>, bodytype=8BITMIME,
proto=ESMTP, daemon=IPv4, relay=msk-m10-st01.rtcomm.ru [213.59.0.34]

Dec 14 14:54:17 aihs sm-mta[5195]: kBEDsGgS005194: to=/dev/null,
ctladdr=bit-bucket (26/0), delay=00:00:01, xdelay=00:00:00, mailer=*file*,
pri=38963, dsn=2.0.0, stat=Sent

Dec 14 14:54:31 aihs sm-mta[5196]: kBEDsTLt005196:
from=<iwmn6@bellsouth.net>, size=7116, class=0, nrcpts=1,
msgid=<6.0.0.22.1.20061214165536.072e7710@bellsouth.net>, proto=SMTP, dae-
mon=IPv4, relay=84-123-178-52.onocable.ono.com [84.123.178.52]

Dec 14 14:54:33 aihs sm-mta[5197]: kBEDsTLt005196: to=fnn@home.fnn,
delay=00:00:03, xdelay=00:00:02, mailer=esmtp, pri=37368, relay=home.fnn.
[80.94.84.26], dsn=2.0.0, stat=Sent (kBEDsZ8K014471 Message accepted for
delivery)
```

Первые три поля каждой записи – это метка времени. Следующие два идентифицируют источник сообщений. Причем эти метки ставятся не генерирующей лог программой («`sendmail`»), а логирующей программой. Оставшаяся часть сообщений принадлежит уже генерирующей программе.

Можно заметить, что записи лога группируются попарно: каждая пара записей имеет одинаковый идентификатор (группа символов после двоеточия, например, «`kBEDsTLt005196`»). Пара записей соответствует двум этапам обработки сообщения электронной почты – прием и отправка.

Далее приведен образец лога веб-сервера «`Apache`» версии 2.1.9-beta. Этот сервер ведет несколько видов логов. Ниже приводится фрагмент лог-файла «`access.log`» – в этом логе фиксируются обработанные запросы протокола HTTP:

```
83.222.198.130 - - [28/Nov/2006:14:46:35 +0300] «GET /cgi-bin/allip_note.pl
HTTP/1.0» 401 475
83.222.198.130 - fnn [28/Nov/2006:14:46:40 +0300] «GET /cgi-
bin/allip_note.pl HTTP/1.0» 500 605
83.222.198.130 - fnn [28/Nov/2006:14:47:27 +0300] «GET /cgi-
bin/allip_note.pl HTTP/1.0» 200 1053
83.222.198.130 - fnn [28/Nov/2006:14:49:10 +0300] «GET /cgi-
bin/allip_note.pl?ip_id=2 HTTP/1.0» 200 2087
83.222.198.130 - fnn [28/Nov/2006:14:49:40 +0300] «GET /cgi-
bin/allip_note.pl?ip_id=3 HTTP/1.0» 200 2087
83.222.198.130 - fnn [28/Nov/2006:14:49:49 +0300] «GET /cgi-
bin/allip_note.pl?ip_id=4 HTTP/1.0» 200 2087
83.222.198.130 - fnn [28/Nov/2006:14:50:05 +0300] «GET /cgi-
bin/allip_note.pl?ip_id=5 HTTP/1.0» 200 2087
83.222.198.130 - fnn [28/Nov/2006:14:56:58 +0300] «POST /cgi-
bin/allip_note.pl HTTP/1.0» 200 1101
83.222.198.130 - fnn [28/Nov/2006:14:57:46 +0300] «POST /cgi-
bin/allip_note.pl HTTP/1.0» 200 1203
83.222.198.130 - - [28/Nov/2006:16:21:58 +0300] «GET / HTTP/1.0» 401 475
83.222.198.130 - amak [28/Nov/2006:16:22:33 +0300] «GET / HTTP/1.0» 200 360
83.222.198.130 - amak [28/Nov/2006:16:22:34 +0300] «GET /cgi-bin/allip.cgi
HTTP/1.0» 404 289
83.222.198.130 - amak [28/Nov/2006:16:23:24 +0300] «GET /cgi-bin/allip-
view.pl HTTP/1.0» 404 293
83.222.198.130 - amak [28/Nov/2006:16:23:34 +0300] «GET /cgi-bin/allip-
view.pl HTTP/1.0» 404 293
83.222.198.130 - amak [28/Nov/2006:16:23:52 +0300] «GET /cgi-bin/allip-
view.pl HTTP/1.0» 404 293
83.222.198.130 - amak [28/Nov/2006:16:24:22 +0300] «GET /cgi-
bin/allip_view.pl HTTP/1.0» 200 1260
83.222.198.130 - amak [28/Nov/2006:16:24:56 +0300] «GET /cgi-
bin/allip_add.pl?instype=ip HTTP/1.0» 200 2481
```

На данном веб-сайте включена авторизация. Как можно видеть, в 1-й и 10-й записях третье поле содержит «-», то есть логин и пароль пользователя не были переданы серверу. Соответственно, код ответа веб-сервера в

этих случаях – 401 (см. предпоследнее поле). Последующие записи уже содержат имя пользователя (в третьем поле – «fnn» и «amak»). То есть, получив в первый раз ответ 401, браузер предлагает пользователю ввести логин и пароль и последующие запросы уже снабжает аутентификационной информацией, отчего они проходят успешно (код 200).

В большинстве записей код ответа веб-сервера 200, что означает успешную обработку. Однако можно заметить коды 500 (внутренняя ошибка сервера) и 404 (страница не найдена).

Последнее поле каждой записи указывает длину ответа веб-сервера в байтах. Как можно заметить, в случае ошибок (401, 404, 500) ответ короткий, а в случае успеха (200) более длинный, поскольку передается веб-страница.

Чтобы верно интерпретировать этот лог, нужно знать значение каждого поля записи. Нетрудно догадаться, например, что первое поле – это IP-адрес клиента, четвертое поле – это время с указанием на часовой пояс. А вот о значении последнего поля догадаться нельзя; о том, что это длина ответа, необходимо знать из документации к веб-серверу.

Лог межсетевого экрана «Netscreen», версия ОС 5.3.0:

```
Dec 14 09:41:09 ns01 moscow-sg2: NetScreen device_id=moscow-sg2  [Root]sys-
tem-notification-00257(traffic): start_time="2006-12-14 09:41:08" duration=0
policy_id=320001 service=icmp proto=1 src zone=Null dst zone=self
action=Deny sent=0 rcvd=540 src=81.16.112.4 dst=81.16.115.162 icmp type=8
session_id=0

Dec 14 09:41:10 ns01 moscow-sg2: NetScreen device_id=moscow-sg2  [Root]sys-
tem-notification-00257(traffic): start_time="2006-12-14 09:41:09" duration=0
policy_id=320001 service=icmp proto=1 src zone=Null dst zone=self
action=Deny sent=0 rcvd=540 src=81.16.112.4 dst=81.16.115.162 icmp type=8
session_id=0

Dec 14 09:41:26 ns01 moscow-sg2: NetScreen device_id=moscow-sg2  [Root]sys-
tem-notification-00257(traffic): start_time="2006-12-14 09:41:22" duration=3
policy_id=2 service=dns proto=17 src zone=Trust dst zone=Untrust
action=Permit sent=90 rcvd=389 src=172.23.36.115 dst=81.16.112.5
src_port=1025 dst_port=53 src-xlated ip=81.16.115.169 port=3975 dst-xlated
ip=81.16.112.5 port=53 session_id=128000

Dec 14 09:41:30 ns01 moscow-sg2: NetScreen device_id=moscow-sg2  [Root]sys-
tem-notification-00257(traffic): start_time="2006-12-14 09:41:24" duration=5
policy_id=2 service=http proto=6 src zone=Trust dst zone=Untrust
action=Permit sent=803 rcvd=1422 src=172.23.69.67 dst=217.212.227.33
src_port=10088 dst_port=80 src-xlated ip=81.16.115.166 port=3982 dst-xlated
ip=217.212.227.33 port=80 session_id=128009

Dec 14 09:41:30 ns01 moscow-sg2: NetScreen device_id=moscow-sg2  [Root]sys-
tem-notification-00257(traffic): start_time="2006-12-14 09:41:23" duration=6
```

```
policy_id=2 service=http proto=6 src zone=Trust dst zone=Untrust
action=Permit sent=455 rcvd=3166 src=172.23.69.67 dst=216.127.68.107
src_port=10087 dst_port=80 src-xlated ip=81.16.115.167 port=3969 dst-xlated
ip=216.127.68.107 port=80 session_id=127975

Dec 14 09:41:30 ns01 moscow-sg2: NetScreen device_id=moscow-sg2  [Root]sys-
tem-notification-00257(traffic): start_time="2006-12-14 09:41:26" duration=3
policy_id=2 service=dns proto=17 src zone=Trust dst zone=Untrust
action=Permit sent=90 rcvd=389 src=172.23.36.115 dst=81.16.112.5
src_port=1025 dst_port=53 src-xlated ip=81.16.115.165 port=3965 dst-xlated
ip=81.16.112.5 port=53 session_id=128000

Dec 14 09:41:30 ns01 moscow-sg2: NetScreen device_id=moscow-sg2  [Root]sys-
tem-notification-00257(traffic): start_time="2006-12-14 09:41:23" duration=6
policy_id=2 service=http proto=6 src zone=Trust dst zone=Untrust
action=Permit sent=1341 rcvd=7164 src=172.23.69.67 dst=217.212.227.33
src_port=10085 dst_port=80 src-xlated ip=81.16.115.168 port=4030 dst-xlated
ip=217.212.227.33 port=80 session_id=127991
```

В этом логе форма представления данных более «человечная», присутствуют метки, позволяющие легко догадаться, к чему относятся приводимые числа. Такие аббревиатуры, как `proto`, `src_port`, `dst_port`, `src-xlated`, говорят специалисту все, что нужно.

Обратите внимание, что в каждой записи присутствуют две метки времени. Одна из них после идентификатора `start_time` ставится генерирующей лог программой (ОС межсетевого экрана), а другая – в начале строки логирующей программой (`syslogd`).

Лог как доказательство

Логи, как правило, не являются непосредственным источником доказательств, но опосредованным. В качестве посредника выступает мнение эксперта или специалиста. Вместо самих логов в качестве доказательств используются: заключение эксперта, заключение специалиста, а также показания изучавших логи свидетелей специалиста, эксперта, понятых. То есть компьютерные логи не являются очевидным доказательством, которое само себя объясняет (такие доказательства, не нуждающиеся в интерпретации, в англоязычной литературе именуют термином «self-evident»). Логи нуждаются в интерпретации.

Автор полагает, что интерпретация логов во всех случаях требует специальных знаний.

Некоторые возражают против доказательности логов, аргументируя это тем, что логи легко фальсифицировать и не существует никакой методики определения истинности логов, отсутствия фальсификации. Это не совсем так [W24].

Во-первых, множество следов других типов фальсифицировать тоже можно. И некоторые – даже проще, чем логи. Волосы, отпечатки зубов,

ворсинки ткани, пороховой нагар и прочее. Не только можно фальсифицировать, но такие попытки регулярно случаются. Несмотря на это, доказательствами все такие следы признаются. Чем логи хуже?

Во-вторых, фальсификацию логов в ряде случаев можно выявить. И чем больше информации в распоряжении эксперта, тем больше вероятность обнаружения подлога.

Цепочка доказательности

Доказательная сила логов базируется на двух столпах – **корректности и неизменности**. А именно – она распадается на следующую цепочку элементов:

1) корректность фиксации событий и генерации записей генерирующей программой;
2) неизменность при передаче записей от генерирующей программы к логирующей программе;
3) корректность обработки записей логирующей программой;
4) неизменность при хранении логов до момента изъятия;
5) корректность процедуры изъятия;
6) неизменность при хранении после изъятия, до осмотра, передачи на экспертизу;
7) корректность интерпретации.

В том случае, когда генерирующая программа сама ведет свои логи (не применяется специализированная логирующая программа), пункт 2 выпадает, а пункты 1 и 3 объединяются.

Подчеркнем, что вышеперечисленные пункты составляют именно цепочку, то есть при выпадении одного звена лишаются опоры последующие звенья. В англоязычной литературе используется термин «custodial chain».

Рассмотрим каждый из пунктов по отдельности и укажем, какие меры обеспечивают действительность каждого из них.

Корректность генерирующей программы

Любая программа может содержать ошибки. Ошибки эти могут возникать спорадически или систематически. В первом случае запись может быть верной или неверной, в зависимости от сочетания случайных или псевдослучайных факторов. Во втором случае ошибка будет носить регулярный характер. Вероятность ошибки в программе зависит от ее производителя. Считается, что она в целом ниже для производителей, применяющих передовые технологии производства программного обеспечения, организовавшими процесс производства в соответствии с современными рекомендациями и сертифицировавшими этот процесс по стандарту ISO-9001. Тем не менее ни у какого производителя вероятность ошибки нельзя считать пренебрежимо малой величиной.

Примеры

В качестве иллюстрации систематических ошибок в логах приведем примеры из практики автора.

Программа «akpop3d» – сервер доставки электронной почты (MDA).

Вот фрагмент лог-файла «maillog», в котором собираются логи как от «akpop3d», так и от сервера электронной почты (MTA) «sendmail»:

```
Dec 12 21:34:28 home sm-mta[4045]: kBCIYOxr004045: from=<chadwicks_coupon@1-
coupon.com>, size=3494, class=0, nrcpts=1,
msgid=<01c71e1c$7a5d7050$6c822ecf@chadwicks_coupon>, proto=ESMTP,
daemon=IPv4, relay=aihs-tun [10.5.0.1]
Dec 12 21:34:39 home sm-mta[4046]: kBCIYOxr004045: to=<fnn@home.fnn>,
delay=00:00:12, xdelay=00:00:11, mailer=local, pri=33713, relay=local,
dsn=2.0.0, stat=Sent
Dec 12 21:38:15 home sm-mta[4051]: kBCIcCrw004051: from=<Most@anderson-
agency.net>, size=49465, class=0, nrcpts=1,
msgid=<000c01c71e1c$a3249630$00000000@eigenaarih63rh>, proto=ESMTP,
daemon=IPv4, relay=aihs-tun [10.5.0.1]
Dec 12 21:38:17 home sm-mta[4052]: kBCIcCrw004051: to=<fnn@home.fnn>,
delay=00:00:03, xdelay=00:00:02, mailer=local, pri=79666, relay=local,
dsn=2.0.0, stat=Sent
Dec 12 21:39:08 home akpop3d[1353]: Connection from 0.80.7.40:1033
Dec 12 21:39:08 home akpop3d[4054]: Authenticated fnn
Dec 12 21:41:01 home akpop3d[4054]: Connection closed
Dec 12 21:45:16 home sm-mta[4076]: kBCIjBAE004076: from=<dhickling@comi-
damexicana.com>, size=5985, class=0, nrcpts=1,
msgid=<000101c71e82$e4adb7ab$9eb3b218@comidamexicana.com>, proto=ESMTP, dae-
mon=IPv4, relay=aihs-tun [10.5.0.1]
Dec 12 21:45:21 home sm-mta[4077]: kBCIjBAE004076: to=<fnn@home.fnn>,
delay=00:00:09, xdelay=00:00:05, mailer=local, pri=36186, relay=local,
dsn=2.0.0, stat=Sent
```

В логе зафиксирован доступ по протоколу POP с адреса 0.80.7.40 (см. строку 5), хотя на самом деле доступ был с адреса 10.0.0.2 (в этом сегменте присутствует вообще единственный клиентский компьютер). Подобная запись повторяется в логе из раза в раз. Очевидно, что в программе «akpop3d» имеется систематическая ошибка, приводящая к некорректной записи в лог. Скорее всего, в программе происходит непредусмотренный побитовый сдвиг или данные считываются по неверному адресу памяти.

Другая иллюстрация систематических ошибок в логах. Операционная система межсетевого экрана «Cisco PIX». Для протокола DNS/UDP вместо номера порта показывается ID запроса. Объявлена в версии 4.4(2), исправлена в версии 6.0(1), идентификатор ошибки (caveats) – «CSCdt72080». Всего в системе учета ошибок (Bug Toolkit) фирмы «Cisco Systems» зарегистрировано 312 ошибок, связанных с логами. Общее число ошибок за весь период жизни ПО – десятки тысяч.

Справедливости ради следует отметить, что ПО «Cisco Systems» пользуется хорошей репутацией и имеет далеко не самое высокое удельное число ошибок, которые к тому же исправно учитываются и своевременно исправляются.

Итак, следует признать, что генерирующая логи программа может допускать ошибки. Однако само по себе это обстоятельство не может служить обоснованием для сомнений[1]. Таковым обоснованием является лишь наличие известной ошибки, которая удовлетворяет одновременно трем условиям:

а) подтверждена службой техподдержки производителя, его уполномоченного представителя (дистрибутора, реселлера) или компетентной организацией, занимающейся учетом ошибок и уязвимостей, либо установлена в результате КТЭ;

б) имеет отношение к генерации логов и может привести к их некорректности, что подтверждается заключением или показаниями эксперта или специалиста;

в) может возникнуть именно в тех записях лога, которые имеют значение для дела, что также должно быть подтверждено заключением или показаниями эксперта или специалиста.

При неисполнении хотя бы одного из трех условий ошибка в программе не является основанием для исключения соответствующего лога из числа доказательств по делу.

Неизменность при передаче

При передаче записей от генерирующей программы к логирующей программе ошибки, приводящие к искажению информации, можно не рассматривать. Их вероятность пренебрежимо мала. Зато не мала вероятность недоставки одной или нескольких записей от генерирующей программы к логирующей. Особенно когда эта доставка происходит по протоколу syslog [55], который не имеет механизма подтверждения приема сообщения.

То есть на этом этапе не следует сомневаться в корректности записи о событии, но стоит предусмотреть возможность пропуска одной или нескольких записей. Особенно если при экспертном исследовании были установлены факты пропуска отдельных сообщений при тех же условиях передачи.

Также целостность лога может быть нарушена при записи в файл. При выключении компьютера методом обесточивания и некоторых других критических ситуациях может произойти сбой файловой операции, в результате чего потеряется одна или несколько последних записей лог-файла.

[1] Имеются в виду не любые сомнения, а именно те сомнения, которые упоминаются в презумпции невиновности (ч. 3 ст. 14 УК).

Корректность логирующей программы

Вероятность ошибки, связанной с искажением записи, весьма мала, хотя и не нулевая. Зато весьма существенной является вероятность ошибки, связанной с меткой времени. Время события может содержаться в самой сгенерированной записи, а может и не содержаться. Эта запись передается логирующей программе, которая обычно добавляет свою собственную метку времени. Часы на разных компьютерах могут показывать разное время. Ошибка в установке часов компьютера может быть небольшой, вследствие естественной их неточности; такая случайная ошибка обычно не превышает 1-3 минут. Она может быть большой вследствие ошибочной установки часов, намеренно сдвинутого времени или путаницы часового пояса; такая регулярная ошибка может исчисляться часами, годами и даже десятилетиями.

В связи с изложенным при осмотре и экспертном исследовании необходимо фиксировать показания часов обоих компьютеров – где работает генерирующая логи программа и где работает логирующая программа.

Неизменность при хранении логов

Логи обычно хранятся в текстовом файле, бинарном файле или базе данных. Собственно процесс хранения не чреват ошибками и искажениями содержания логов. Следует учитывать лишь два фактора: возможную намеренную фальсификацию логов каким-либо лицом и уничтожение некоторых записей по истечении установленного срока хранения.

Поэтому во время изъятия логов или при изучении их экспертом необходимо отметить права доступа на запись для различных пользователей, а также настройки систем хранения, ротации и чистки логов.

Сомнения по поводу намеренного искажения логов не могут возникнуть лишь в силу существования само́й технической возможности их искажения. Для обоснованности сомнений требуется наличие признаков, свидетельствующих о факте доступа на запись к логам.

Корректность изъятия

Когда логи осматриваются и изымаются «на месте», без передачи компьютера целиком на экспертизу, возможны следующие ошибки.

Логи могут иметь достаточно большой размер – миллионы записей и больше. Просмотреть глазами и распечатать на бумаге такие логи невозможно. Для их просмотра приходится применять фильтры, например, программу «`grep`». Задать «фильтрующие» выражения – задача простая лишь на первый взгляд. Здесь легко ошибиться даже для специалистам.

Например, мы осматриваем лог веб-сервера «`Apache`». Сервер активно используется в основном локальными пользователями из сети `10.0.0.0/16`. Есть сведения, что злоумышленник осуществлял несанкционированный доступ к этому серверу, используя IP-адрес из другой сети, какой именно, неизвестно. В суточном логе пара сотен тысяч записей, и просмотреть или распечатать его целиком нельзя.

Участвующий в осмотре специалист, особенно не задумываясь, набирает команду, которая на первый взгляд очевидна. Она должна отфильтровать обращения со всех местных IP-адресов, начинающихся на «`10.0.`», оставив только «чужие» IP-адреса:

```
grep -v " 10.0." /data/apache/logs/access.log
```

(показать все записи лога, кроме тех, где встречается подстрока, указанная в кавычках; перед «10» поставлен пробел, чтобы не попали записи, где «10» – это второй или третий октет IP-адреса).

В результате происходит незамеченная, но фатальная ошибка! Не обнаруженными оказываются все записи, в которых метка времени соответствует заданному шаблону. То есть все записи в период с 10:00:00 до 10:09:59. В эти-то десять минут злоумышленник и осуществил свой доступ. Специалист забыл, что в шаблоне команды «`grep`» символ «.» означает не точку, а любой одиночный символ.

Эту ошибку можно обнаружить постфактум, если в протоколе осмотра точно воспроизведена примененная команда. Эту ошибку можно не только обнаружить, но и исправить, если кроме распечатки выдержки из лога полный лог был скопирован на компакт-диск и приложен к протоколу.

Логи могут храниться в нескольких местах, например, в нескольких файлах. Причем содержимое разных лог-файлов может (а) совпадать, (б) являться подмножеством одно другого, (в) частично пересекаться, (г) взаимно дополнять друг друга без пересечения. Поэтому при изъятии следует зафиксировать настройки, отвечающие за распределение записей по местам хранения. Также важно не упустить какой-либо лог, который может храниться в нестандартном месте.

В протоколе осмотра должны быть указаны сведения, относящиеся как к корректности, так и к полноте осмотра. То есть желательно описать все возможные места хранения логов, привести настройки программ, отвечающих за их хранение, осмотреть и приложить к протоколу в бумажном виде наиболее существенные записи, а все прочие логи, программы, настройки в полном объеме скопировать на диск и приложить к протоколу.

Когда есть такая возможность, лучше произвести полное копирование всего содержимого жесткого диска на самом низком из возможных уровней. Например, при помощи программы «dd» или специальным аппаратным дупликатором дисков.

Неизменность после изъятия

Изъятые логи либо распечатываются на бумаге и прилагаются к протоколу, либо записываются на компьютерный носитель, который опечатывается и хранится в деле. Лучше совместить оба способа: наиболее существенные записи лога распечатать, а лог целиком записать на компакт-диск.

Еще одной гарантией корректности осмотра логов и неизменности информации после изъятия является участие в следственном действии специально подобранных понятых. В соответствии с УПК понятой призван удостоверить факт производства следственного действия, а также его содержание, ход и результаты (ст. 60 УПК). Для тех действий, которые проводятся **непосредственно**, понятой не должен обладать какими-то особенными свойствами, кроме исправности зрения, слуха, а также дееспособности. Но действия с компьютерной информацией проводятся отнюдь не непосредственно, а при посредстве разнообразных технических средств. Для применения этих технических средств, разумеется, нужен специалист. Но понятые также должны понимать смысл проводимых действий, их содержание и последствия. Рекомендуется для участия в таких следственных действиях привлекать понятых, обладающих познаниями относительно осматриваемых аппаратных и программных средств, о чем сделать запись в протоколе.

Корректность интерпретации

В ряде случаев записи лога интерпретируются следователем. Иногда спрашивают совета специалиста.

Вспоминается случай, когда материал относительно неправомерного доступа принесли одному генералу. Бо́льшую часть материалов составляли разнообразные логи. Также были приложены распечатки записей из базы данных RIPE (регистратора IP-адресов) относительно встречавшихся в логах IP-адресов. Посмотрев бумаги с умным видом, генерал приказал задержать и допросить хакера. Когда опер ему возразил, что злоумышленник пока еще не установлен, генерал заявил, что доказательства, конечно, еще предстоит собрать и оформить, но мы-то хакера уже знаем: вот в логах его фамилия, адрес и телефон – и ткнул пальцем в запись типа «`person`» в распечатке из `whois`.

Автору представляется, что интерпретация лога как такового, без предварительного ознакомления с программами, его создавшими и обработавшими, а также их настройками – некорректна. Поэтому следует документировать не только сами логи, но также имеющие к ним отношение программы, их настройки и окружение. Кроме того, следует получить мнение специалиста или эксперта относительно интерпретации логов на основании вышеуказанной информации.

Процедура приобщения логов

Итак, на основании вышеописанной «цепочки доказательности логов» дадим рекомендации по процедуре получения и приобщения к делу соответствующих доказательств.

Предположим, имеются основания считать, что на известном сервере в логах зафиксированы события, связанные с преступлением и позволяющие установить и изобличить преступника. Как провести следственные действия?

Понятно, что нет возможности доказать отсутствие всех ошибок во всех программах и настройках, нет возможности доказать отсутствие любых фальсификаций со стороны любых лиц. Однако это не означает, что следует удариться в противоположную крайность и вовсе никак не проверять и не удостоверять корректность и неизменность информации из логов. Вредны обе крайности – как вообще не проверять условий и окружения, так и требовать полного аудита безопасности осматриваемого сервера.

Степень строгости и подробности зависит от возможностей следствия и от судебной практики. Автор предлагает три варианта, отличающиеся строгостью доказывания – нестрогий, промежуточный и строгий. Назовем их соответственно.

Деревенский вариант

Следователь или оперуполномоченный совместно со специалистом (из числа сотрудников, обслуживающих осматриваемый сервер) и понятыми проводит осмотр содержимого сервера. При этом используются штатные программные и аппаратные средства. Составляется протокол осмотра, где отражается следующее:

- характеристики сервера, версия ОС;
- наличие и рабочее состояние программы генерирующей и программы, обрабатывающей логи;
- наличие файлов с логами, их временны́е метки;
- права доступа к лог-файлам;
- учетные записи (аккаунты) пользователей, имеющих права на запись в лог-файлы.

Нужные записи из нужных логов выбираются при помощи соответствующих фильтров, распечатываются на принтере и прилагаются к протоколу осмотра.

Все листы протокола и приложений подписываются участниками осмотра.

Провинциальный вариант

Для участия в следственном действии приглашается независимый специалист. Представитель владельца сервера (желательно из числа тех-

нических сотрудников) также участвует в осмотре. Понятые приглашаются не любые, а квалифицированные. В протоколе делается запись, что «понятые имеют необходимую квалификацию в области ИТ, знания по осматриваемой технике и ПО и поэтому полностью понимают смысл всех производимых в ходе осмотра действий».

Помимо указанных в предыдущем варианте данных также собираются и отражаются в протоколе следующие:

- сведения о защищенности системы, ее проверке на наличие вредоносных программ, сведения об установленных обновлениях (патчах*);
- подробные данные о генерирующей логи программе, всех ее настройках и окружении (чтобы можно было узнать о выявленных ошибках и оценить вероятность невыявленных);
- данные о протоколе и параметрах передачи логов от генерирующей программы к логирующей;
- подробные данные о логирующей программе, в том числе настройки касательно размещения, срока хранения и ротации логов;
- сведения, помогающие интерпретировать логи, например, описания используемых программ.

Существенные записи из логов выбираются и в печатном виде прилагаются к протоколу. При этом полные логи, задействованные программы и их настройки копируются на компакт-диск типа CD-R или DVD-R (однократная запись), который опечатывается и в случае необходимости отправляется на экспертизу.

Столичный вариант

При участии следователя, квалифицированных понятых, специалиста и представителя владельца сервера нужный сервер отключается, опечатывается должным образом (см. главу «Тактика обыска») и отправляется на экспертизу.

Перед экспертом ставятся вопросы касательно содержания логов, их интерпретации, а также вопросы об известных ошибках, приводящих к некорректности логов, о защищенности системы, о следах возможной фальсификации или несанкционированного удаления логов.

Переносной дупликатор жестких дисков «ImageMASSter Solo-3 IT». Позволяет снять полную, пригодную для экспертного исследования копию содержимого НЖМД прямо на месте происшествия. Поддерживает интерфейсы IDE (ATA), SATA и SCSI

Снятие копии диска

В качестве альтернативы изъятию сервера целиком возможно снятие на месте полной копии его дисков при помощи специализированного аппаратного устройства или программным способом. Копия диска или образ диска (конечно, имеется в виду побитовая копия, «сектор в сектор», «bitstream image») затем передается на экспертизу с такими же вопросами, как если бы передавался сам диск.

Существует несколько моделей аппаратных дупликаторов жестких дисков и несколько программных. К программным относятся «EnCase», «FTK», «SMART», «dd» и его вариации («dd_rescue», «DCFLDD» и др.), «NED». Самый простой из программных дупликаторов – это программа «dd», входящая в состав любой операционной системы класса Unix/Linux.

Естественно, для снятия копии диска надо иметь с собой жесткий диск или несколько дисков суммарной емкостью не меньше, чем копируемый диск.

Копию диска осматриваемого компьютера на месте происшествия можно сделать четырьмя способами:

- из выключенного компьютера извлечь НЖМД, подключить его к компьютеру специалиста (желательно смонтировать в режиме read-only или подсоединить через аппаратный блокиратор записи) и программными средствами, имеющимися на компьютере специалиста, сделать копию;
- из выключенного компьютера извлечь НЖМД, подключить его к аппаратному автономному устройству для дупликации дисков и сделать копию;
- к осматриваемому компьютеру подключить дополнительный НЖМД или иное внешнее устройство и скопировать информацию на него, воспользовавшись программными средствами, имеющимися на осматриваемом компьютере, а лучше – средствами, принесенными специалистом;
- установить с осматриваемого компьютера сетевое соединение с удаленным компьютером (сервером) специалиста и скопировать образ диска туда по сети, воспользовавшись программными средствами, имеющимися на осматриваемом компьютере, а лучше – взятыми с удаленного сервера.

Выбор способа предпочтительно оставить на усмотрение специалиста. При выборе он будет исходить не только из имеющихся в распоряжении средств, но и принимать во внимание другие обстоятельства. Например, насколько вероятно наличие на осматриваемом компьютере руткита* или логической бомбы*, какие последствия повлечет остановка работы исследуемого компьютера и т.п.

Стерильность

В случае, когда копирование дисков производится по схеме «сектор в сектор», очень важно, чтобы целевой диск (на который копируется) был предварительно очищен. То есть все его сектора без исключения должны быть перезаписаны нулями или случайными байтами. В противном случае эксперт, думая, что исследует копию одного диска, на самом деле найдет там остатки предыдущей копии, которые не сможет различить. То, что все сектора целевого диска предварительно очищены, должно быть зафиксировано в протоколе.

Следует помнить, что не все программы, предназначенные для «очистки диска», корректно выполняют свою функцию. Даже не говоря о случаях наличия ошибок и недоработок в программе. Такая программа может не поддерживать (или не вполне корректно поддерживать) текущую файловую систему. Программы, работающие из-под ОС «Windows», могут просто не получить доступ к некоторым областям диска по воле ОС или драйвера. Бывает, что ОС переадресует обращения к некоторым секторам диска на другие секторы. В результате диск очистится не полностью. Для постоянного использования на своем компьютере с целью, например, обеспечения приватности это не страшно. Но для «стерилизации» диска, на который предполагается копировать информацию для последующего исследования, это неприемлемо. Для полной очистки следует применять программы под ОС DOS или UNIX.

В случае, когда копирование дисков производится по схеме «диск в файл», предпринимать меры по предварительной очистке целевого диска не обязательно.

Для той же цели – застраховаться от возможной «нестерильности» целевого диска – при копировании полезно вычислять хэш-функции или контрольные суммы копируемых секторов (групп секторов) и заносить их в протокол. В дальнейшем эксперт может перевычислить значение этих функций для исследуемой копии и тем самым убедиться в ее точности.

Тактика обыска

Когда искомые доказательства могут содержаться на компьютерных носителях, обыск следует проводить согласно нижеизложенным правилам, чтобы обеспечить законность и доказательную силу.

К компьютерным носителям информации относятся съемные и несъемные магнитные диски, компакт-диски (CD), DVD-диски, флэш-накопители, оптические диски, магнитные карты, цифровые кассеты и некоторые другие. Такие носители могут содержаться в персональных компьютерах, серверах, коммуникационном оборудовании, наладонных компьютерах (КПК, PDA), коммуникаторах, смартфонах, мобильных телефонах, цифровых фотоаппаратах и видеокамерах, плеерах и иной другой подобной технике – вся такая техника со встроенными носителями изымается целиком.

Другие виды техники не содержат доступных пользователю носителей компьютерной информации, поэтому ее изымать или исследовать не обязательно. Таковыми являются: принтеры, сканеры, факс-аппараты, а также клавиатуры, мониторы, мыши, джойстики, звуковые колонки. Следует помнить, что техника стремительно развивается и доступные пользователю носители могут завтра появиться в составе таких устройств, какие еще сегодня их не имеют. Стоит вспомнить, например, что в 2000 году аудиоплеер не следовало рассматривать как носитель компьютерной информации, а ныне почти все аудиоплееры (MP3-плееры) по совместительству являются пользовательскими переносными накопителями. В ближайших планах производителей оснастить встроенными компьютерами всю бытовую технику – холодильники, кондиционеры, кофеварки, стиральные машины и т.д. Компьютер в составе бытовой техники, скорее всего, будет включать встроенный или съемный носитель и сетевой интерфейс для удаленного доступа.

Итак, для начала изложим базисные принципы обращения с информносителями и компьютерной техникой при проведении обыска, а затем более подробно опишем правила проведения обыска при наличии такой техники.

Принципы

1. Во время изъятия компьютерной техники не должна изменяться никакая содержащаяся на изымаемых носителях информация. На следствии лежит обязанность доказать, что представленная эксперту или суду компьютерная информация не изменялась. Ни в процессе обыска, ни при последующем хранении.

2. Доступ к информации и исследование ее «на месте» допустимы лишь в тех случаях, когда невозможно изъять носитель и отправить его на экспертизу. Такой доступ должен производиться компетентным специалистом, который в состоянии понять и объяснить смысл и все последствия производимых им действий.

3. Должны протоколироваться все действия с компьютерной техникой так, чтобы независимый исследователь мог бы их повторить и получить такие же результаты.

Общие правила изъятия компьютерной техники при обыске

1. Возьмите под контроль помещение, где установлена техника, а также электрощит. Не позволяйте никому, кроме вашего специалиста, дотрагиваться до техники и устройств электропитания. В крайнем случае, ес-

ли отстранить местный персонал от техники невозможно, фиксируйте все их действия.

В тех редких случаях, когда есть основания полагать, что о проведении обыска известно расторопным сообщникам, находящимся вне вашего контроля, то как можно скорее следует отключить сетевые соединения компьютеров. Для этого вытащить из компьютеров кабели локальной сети и отключить модемы. За те несколько минут, пока фотографируют и подготавливают к выключению технику, сообщник, в принципе, может успеть соединиться по сети с компьютером и уничтожить на нем существенную информацию.

2. Выключенные устройства не включайте.

3. Сфотографируйте или снимите на видео компьютерную технику. В крайнем случае, можно зарисовать схему. Уделите внимание кабелям – какой куда подключен. Подключение кабелей также желательно сфотографировать или снабдить их ярлыками для идентификации мест подключения. Всю подключенную к компьютеру периферию следует сфотографировать и/или описать в протоколе, чтобы было ясно, как все было соединено.

4. Если на момент обыска компьютер включен, сфотографируйте или иным образом зафиксируйте изображение на мониторе.

С включенным, но «спящим» компьютером можно поступить двояко: либо сразу, не трогая его, выключить, как описано ниже, либо сначала активизировать, слегка сдвинув мышь, сфотографировать содержимое экрана, а уже затем выключить. Выбор варианта остается за руководителем операции. При «пробуждении» или активизации компьютера может оказаться, что выход из «спящего» режима или из скринсейвера* защищен паролем. Тогда после сдвигания мыши вместо содержимого экрана вы увидите запрос пароля. В таком случае компьютер надо выключить описанным ниже способом.

5. Найдите и соберите листочки, на которых могут быть записаны пароли, сетевые адреса и другие данные, – часто такие записи лежат на рабочем месте, приклеены к монитору, висят на стене.

6. Если принтер что-то печатает, дождитесь окончания печати. Все, что находится в выходном лотке принтера, описывается и изымается наряду с другими носителями компьютерной информации.

7. После этого компьютеры надо выключить. Это должен сделать компетентный специалист. Не позволяйте делать это местному персоналу или владельцу изымаемой техники, не принимайте их советов. Если с вами нет специалиста, выключение настольного компьютера следует производить вытаскиванием шнура питания из корпуса компьютера (не из стенной розетки). Выключение ноутбука следует производить вытаскиванием электрического шнура и извлечением его аккумулятора без закрывания крышки.

Иногда можно ошибиться, приняв включенный компьютер за выключенный. При гибернации («засыпании») экран гаснет, приостанавливаются некоторые функции компьютера. Могут погаснуть или изменить цвет светодиодные индикаторы. Тем не менее у включенного, хотя и «заснувшего» компьютера обязательно горит индикатор питания на системном блоке. У выключенного, напротив, все индикаторы на системном блоке погашены, хотя может гореть индикатор на мониторе. Подробнее о выключении – в параграфе «Как выключать?» главы «Короткоживущие данные».

8. Техника опечатывается таким образом, чтобы исключить как физический доступ внутрь корпуса, так и подключение электропитания. Это обстоятельство отражается в протоколе.

9. Изъятая техника упаковывается сообразно с хрупкостью и чувствительностью к внешним воздействиям. Особо чувствительны к вибрации жесткие магнитные диски (НЖМД); их механическое повреждение (например, из-за перевозки в багажнике) приводит к полной недоступности данных.

10. Опросите всех пользователей на предмет паролей. Надо постараться узнать у каждого сотрудника все известные ему пароли (точнее, пары логин-пароль), имеющие отношение к изъятой технике. Пароли не следует воспринимать на слух. Их надо записать по символам, обращая внимание на алфавит и регистр каждого символа и выверить у источника. Пароли допустимо не вносить в протокол допроса или объяснение, а записать просто на бумажке. Их доказательное значение от этого не снижается.

Особенности

Относящаяся к делу компьютерная информация и иные цифровые следы криминальной деятельности могут содержаться во множестве цифровых устройств и носителей. Во время обыска нужно постараться обнаружить все такие устройства и носители, быстро решить, может ли в них содержаться интересующая информация, и изъять их, если может.

Для обнаружения таких носителей или устройств необходимо участие специалиста.

На случай, когда специалиста нет, на последующих иллюстрациях приведены наиболее распространенные устройства, могущие содержать в себе компьютерную информацию.

Ниже приводятся рекомендации по обращению с некоторыми видами компьютерной техники. Ими следует руководствоваться только при отсутствии в вашей группе технического специалиста. Специалист должен знать, как следует обращаться с каждой конкретной моделью техники, чтобы сохранить информацию в неизмененном виде. В присутствии специалиста надо следовать его указаниям.

Ноутбук (лэптоп, переносной компьютер)

Если ноутбук включен на момент начала обыска, то прежде всего следует сфотографировать или иным образом зафиксировать содержимое экрана, как это указывалось выше.

Чтобы выключить ноутбук, недостаточно вытащить из него шнур питания; при этом ноутбук перейдет на питание от аккумулятора. Для обесточивания надо извлечь аккумулятор. При этом не следует закрывать крышку ноутбука, складывать его. При складывании обычно активизируется функция гибернации («засыпания»), а это означает внесение изменений в информацию на диске, что нарушит вышеозначенные принципы.

Наладонный компьютер (КПК)

К данному классу относятся: КПК, PDA (Personal Digital Assistant), palmtop, pocket PC, органайзеры, смартфоны, коммуникаторы, электронные дневники [51, 84, 93].

Особенностью этого класса компьютеров является то, что значительная часть пользовательских данных хранится у них в оперативной, энергозависимой памяти. При отключении питания наладонника вся такая информация безвозвратно пропадет.

Штатное состояние «выключен» у наладонника фактически означает не выключение, а режим «засыпания» или гибернации. При этом электроэнергия расходуется только на поддержание оперативной памяти. Храниться в таком состоянии он может до нескольких дней, в зависимости от текущего состояния аккумулятора.

Наладонный компьютер, сменный модуль памяти (SD), крэдл и стило к нему

Если наладонник включен (активен) на момент начала обыска, то прежде всего следует сфотографировать или иным образом зафиксировать содержимое экрана, как это указывалось выше. При неактивности экран автоматически гаснет, а наладонник переходит в режим гибернации через

несколько минут. После фотографирования можно выключить его вручную кнопкой «power», если есть такая кнопка.

Касаться экрана наладонника нельзя, поскольку экран у него является чувствительным; каждое прикосновение к экрану воспринимается как команда.

Извлекать аккумулятор из наладонника нельзя.

Вместе с ним обязательно следует изъять крэдл (подставку с устройством питания и сопряжения) либо иное зарядное устройство. Хранить наладонник сам по себе, без подзарядки, можно недолго, обычно несколько дней. Длительность хранения зависит от первоначального состояния аккумулятора. После его истощения содержимое оперативной памяти будет утрачено. Лучше не рисковать и после изъятия как можно быстрее передать компьютер эксперту. А до такой передачи, по возможности, хранить его вставленным в крэдл, чтобы аккумулятор не истощался. В крэдле (который, естественно, должен быть подключен к электросети) хранить наладонник можно неограниченно долго. Правда, хранение в крэдле несовместимо с опечатыванием компьютера.

В протоколе обыска (изъятия, личного досмотра) следует указать примерно следующее: «При осмотре и изъятии наладонного компьютера его кнопки не нажимались, экрана не касались, аккумулятор или съемные накопители не извлекались. Наладонный компьютер в состоянии гибернации (засыпания) был упакован и опечатан так, чтобы исключить всякий доступ к органам его управления (клавиши, экран) и к его разъемам без повреждения печатей».

Принтеры

Современные принтеры (за очень редким исключением) не имеют доступных пользователю носителей компьютерной информации. Поэтому изымать принтеры нет необходимости. Надо только изъять все распечатки, обнаруженные в выходном лотке принтера или подле него, поскольку такие распечатки также содержат компьютерную информацию. Кроме того, некоторые фотопринтеры имеют разъем для непосредственного подключения носителей информации типа флэш-накопителей. Если такой накопитель оставлен в разъеме принтера, его нужно изъять, а принтер можно не трогать. При проведении осмотра или обыска следует отразить в протоколе наличие принтера и способ его подключения к компьютеру.

Из этого правила есть одно исключение – дела о подделке документов.

Принтеры очень часто используются для изготовления поддельных документов, поскольку их разрешающая способность (от 600 точек на дюйм и больше) превышает разрешающую способность человеческого глаза. То есть фальшивку, отпечатанную на современном принтере, отличить на глаз нельзя.

Экспертиза может установить, что поддельный документ был напечатан именно на этом конкретном принтере или с использованием конкретного картриджа.

Когда в деле фигурируют поддельные документы, то кроме компьютеров и машинных носителей информации следует также изымать:

- принтеры;
- картриджи для принтеров (кроме, может быть, новых в упаковке) и иные расходные материалы (тонер, ленты, чернила);
- все обнаруженные распечатки;
- чистую бумагу и пленку, приготовленные для использования в принтере.

Принтер следует опечатать так, чтобы сделать невозможным подключение электропитания и доступ к печатающему узлу без нарушения упаковки. Этот факт отразить в протоколе. Иные изъятые материалы также следует опечатать.

Сканеры

В сканерах так же, как и в принтерах, нет доступных носителей информации. Изымать их нет смысла.

К сожалению, нет возможности установить, было ли то или иное изображение (скан-копия) получено с конкретного сканера.

При проведении осмотра или обыска следует лишь отразить в протоколе наличие сканера и способ его подключения к компьютеру.

Флэш-накопители

Накопители на флэш-памяти выпускаются в виде самостоятельных устройств, а также в составе других устройств, таких как аудиоплееры или цифровые фотоаппараты. Форма и размер устройств с флэш-накопителями также весьма разнообразны. Чаще всего такие накопители снабжены интерфейсом типа USB, по которому их и можно опознать.

Такие накопители не теряют данные при отсутствии электропитания, поэтому их можно хранить долгое время. При изъятии следует опечатать так, чтобы исключить доступ к USB-разъему и органам управления (если такие органы есть).

Флэш-накопитель в виде брелка

Снять копию флэш-накопителя на месте, в принципе, можно. Как это сде-

Флэш-накопитель в составе аудиоплеера

Флэш-накопитель в часах

Электронная фоторамка со встроенным флэш-накопителем

лать, рассказано в разделе «Компьютерно-техническая экспертиза». Но особенной необходимости в таком копировании нет, поскольку флэш-накопитель все равно изымается, когда есть основания полагать, что на нем может содержаться существенная для дела информация. Затем он передается на экспертизу. Снимать копию на месте логично в тех случаях, когда ждать результатов экспертизы нет времени и нужно быстро получить информацию для продолжения расследования. В таких случаях специалист снимает копию с накопителя на месте, сам накопитель опечатывается, изымается и откладывается ждать экспертизы, а его копия подвергается исследованию с целью получения неофициальной, зато срочной информации.

Мобильные телефоны

Перед тем, как рассмотреть изъятый мобильный телефон в качестве носителя компьютерной информации, следует решить, требуется ли получить с него материальные следы – отпечатки пальцев, следы наркотиков, иные.

Следует помнить, что некоторые методы снятия отпечатков могут привести телефон в негодность.

В большинстве случаев при изъятии нужно выключить мобильный телефон, чтобы исключить потерю имеющихся данных вследствие поступления новых вызовов и новых SMS. Аккумулятор вынимать не следует.

Однако в некоторых случаях руководитель операции может решить, что контролировать поступающие вызовы важнее. Тогда телефон надо оставить включенным и подзаряжать его по мере необходимости.

Выключенный телефон упаковывается в жесткую упаковку и опечатывается так, чтобы исключить доступ к органам его управления. Это отмечается в протоколе.

При выключении телефона не надо беспокоиться о PIN-коде на доступ к данным в SIM-карте телефона. У оператора связи в любой момент можно узнать PUK (PIN unlock key) и с его помощью получить доступ к SIM-карте.

О полевом и лабораторном исследовании информации из мобильных телефонов есть достаточно много технической литературы [60].

Коммутаторы и маршрутизаторы

Обычно коммутатор* (switch) имеет внутреннюю энергонезависимую память, в которой помещается только операционная система и файл конфигурации. Именно конфигурация может быть предметом интереса следствия. Мелкие коммутаторы могут не иметь доступной пользователю памяти, хотя свою конфигурацию (настройки) все же сохраняют. Совсем мелкие коммутаторы для домашнего использования и хабы могут не иметь даже настроек.

Маршрутизатор* (router), в зависимости от своего назначения, может иметь столь же небольшую память, как и коммутатор, где хранится лишь относительно небольшой файл конфигурации, а может иметь и более существенное устройство хранения, например, жесткий диск.

Конфигурация маршрутизатора или коммутатора может заинтересовать следствие лишь при некоторых специфических типах преступлений. В большинстве случаев их конфигурация не представляет интереса.

Снять всю конфигурацию с маршрутизатора или коммутатора специалист может на месте, если знать пароль для доступа.

Включенные коммутаторы и маршрутизаторы следует при изъятии отключать вытаскиванием электрического шнура либо аппаратным переключателем (рубильником), который находится прямо на встроенном блоке питания.

Автомобильные компьютеры

Бортовым компьютером оснащены практически все современные модели автомобилей. Основное его предназначение – оптимизация режима двигателя с целью экономии горючего. Компьютер собирает многочисленные данные с различных устройств автомобиля. В случае аварии в нем можно найти сведения о нескольких последних секундах – скорость, обороты, позиции педалей газа и тормоза, режим стеклоочистителей, осветительных приборов и т.п.

Образец автомобильного навигационного компьютера

Кроме того, бортовой компьютер выполняет навигационные функции либо для этого установлен отдельный навигационный компьютер. В нем фиксируется расположение автомобиля в разные моменты времени, вычисляются возможные маршруты следования до заданных точек.

К сожалению, бортовые компьютеры не унифицированы, как персональные. Расположение компьютера и его запоминающего устройства зависит от модели автомобиля. Для изъятия или копирования носителей компьютерной информации следует пригласить специалиста из фирменного (авторизованного) центра техобслуживания соответствующего автопроизводителя.

Модемы

В некоторых модемах хранится пользовательская информация – настройки сети или телефонные номера провайдера. Если нет специалиста, который может указать, какая именно модель модема здесь присутствует – с памятью или без, – то модем надо отключить от электропитания, опечатать и изъять.

Цифровые фотоаппараты

Практически все цифровые фотоаппараты (фотокамеры) имеют сменный и встроенный накопитель достаточно большой емкости. Этот накопитель доступен пользователю не только для чтения, но и для записи. Поэтому кроме отснятых фотографий и видеороликов там можно найти и иную пользовательскую информацию. Иногда цифровой фотоаппарат используется в качестве переносного USB-накопителя.

Цифровые фотоаппараты могут иметь форму как традиционную, так и непривычную

Сменные накопители

Есть несколько стандартных типов таких накопителей. Это ныне уже устаревшие и выходящие из употребления гибкие магнитные диски (ГМД) или дискеты, магнитооптические диски, компакт-диски (CD), DVD-диски, сменные флэш-карты, а также НЖМД, выполненные в отдельном корпусе.

Различные типы сменных накопителей на основе флэш-памяти

Короткоживущие данные

В этой главе мы рассмотрим, как специалист при проведении следственного действия должен обращаться с короткоживущими, или волатильными данными. Этим термином обычно именуют такую информацию, которая недолговечна и существует лишь до момента выключения компьютера или до завершения определенной программы.

Перечень

Вот некоторые из типов короткоживущих данных:

- содержимое ОЗУ*, то есть все исполняемые в текущий момент программы (задачи, процессы), системные и прикладные (пользовательские);
- прежнее содержимое ОЗУ в областях оперативной памяти, которые на текущий момент считаются свободными;
- список открытых файлов со сведениями, какой процесс каким файлом пользуется;
- информация о пользовательских сессиях, то есть вошедших в систему (залогиненных, зарегистрированных) пользователях;
- сетевая конфигурация – динамически присвоенный IP-адрес, маска подсети, ARP-таблица, счетчики сетевых интерфейсов, таблица маршрутизации;
- сетевые соединения – информация о текущих соединениях (коннекциях) по различным протоколам, о соответствующих динамических настройках межсетевого экрана* или пакетного фильтра;
- текущее системное время;
- список назначенных заданий (scheduled jobs);
- кэш доменных имен и NETBIOS-имен;
- загруженные модули ядра (LKM);
- монтированные файловые системы, подключенные сетевые диски;
- файл или область подкачки* (swap-файл) на диске – информация о текущем состоянии виртуальной части ОЗУ, а также ранее находившиеся там данные;
- временные файлы, которые автоматически стираются при штатном завершении работы ОС или при загрузке ОС.

Все перечисленные данные, кроме последних двух пунктов, хранятся в ОЗУ.

Кроме того, к короткоживущим данным можно причислить образцы сетевого трафика* в обоих направлениях – с исследуемого компьютера и на него. Проанализировать устройство и функции программы по содержимому ОЗУ (дампу памяти*) бывает довольно сложно. Зато по генерируемому программой трафику во многих случаях нетрудно определить ее

функции. Поэтому образец трафика компьютера за какой-то разумный период времени будет хорошим дополнением для исследования работы неизвестных программ.

Понятно, что короткоживущие данные (кроме области подкачки*) можно снять лишь с работающего компьютера. После выключения все такие данные будут утрачены. То есть снятие короткоживущих данных производится не экспертом при проведении КТЭ, а специалистом во время следственного действия. Исключение – экспертиза КПК* (наладонного компьютера), который обычно хранится во включенном состоянии, но в режиме гибернации*.

Стоит ли пытаться снять с работающего компьютера короткоживущие данные? С одной стороны, среди них могут оказаться полезные и даже очень ценные, например, запись о текущей TCP-сессии с атакуемым узлом или ключ для доступа к криптодиску*. С другой стороны, при снятии содержимого ОЗУ невозможно не изменить информацию на компьютере, в том числе на его диске. Это может отрицательно повлиять на оценку достоверности последующей экспертизы. В каждом случае это решает специалист, оценивая, какой аспект важнее для дела – сохранность долгоживущей информации или возможность получить короткоживущую критичную. Разумеется, для этого специалист должен быть проинформирован о существенных обстоятельствах дела.

Например, при использовании подозреваемым криптодиска получить доступ к его содержимому можно либо как-то узнав пароль, либо застав компьютер во включенном состоянии с активированным (монтированным) криптодиском. После демонтирования криптодиска узнать пароль непросто. В практике автора было несколько случаев, когда у подозреваемого удавалось выяснить пароль к его криптодиску путем изощренного обмана или примитивного запугивания. Однако грамотный в области ИТ пользователь знает четко: если он не сообщит пароль, то расшифровать данные на криптодиске невозможно. Остается второй способ. Надо каким-то образом прорваться к включенному компьютеру и, пока доступ к криптодиску открыт, снять с него все данные или извлечь из ОЗУ ключ шифрования.

Стоит ли пытаться снять короткоживущую информацию, рискуя при этом существенно изменить данные на нем или сразу выключить компьютер, – решает специалист, исходя из материалов дела.

В любом случае, настоятельно рекомендуется снять минимально возможную без риска короткоживущую информацию – сфотографировать или описать текущее изображение на экране включенного компьютера.

Снятие

Для сбора короткоживущей информации из ОЗУ и свопа* есть различные программные инструменты под различные ОС. Специалисту предпочтительно не надеяться, что такие инструменты найдутся на исследуемом компьютере, а пользоваться своими собственными программами, которые заранее приготовлены на дискете, компакт-диске или флэш-накопителе. Чаще всего используют компакт-диск.

Кроме того, следует приготовить еще один носитель – для записи результатов снятия короткоживущей информации. Предпочтителен флэш-накопитель. Для сброса результатов вместо флэш-накопителя или иного устройства можно подключить в качестве сетевого диска диск удаленного компьютера. Таковым может служить переносной компьютер специалиста, принесенный им с собой и подключенный к тому же сегменту ЛВС, или стационарный компьютер специалиста, доступный через Интернет. Сбрасывать полученные короткоживущие данные на жесткий диск исследуемого компьютера категорически не рекомендуется. Этим можно уничтожить некоторую существенную для дела информацию и поставить под сомнение результаты последующей экспертизы.

Корректность работы программных инструментов по снятию информации с работающего компьютера зависит не только от самих этих инструментов. На результат может влиять также состояние исследуемого компьютера. Например, если он заражен вредоносной программой типа руткит*, то специалист может и не получить корректную информацию, даже при безупречной работе его инструментов.

Вот некоторые полезные программы для сбора короткоживущих данных:

- Утилиты «PMDump», «userdump», «dd» позволяют снимать содержимое ОЗУ компьютера (дамп памяти). Запуск любой программы изменяет содержимое ОЗУ, поэтому результат работы таких утилит будет не вполне «чистый». Но это неизбежная погрешность.
- Утилиты «ifconfig», «ipconfig», «arp», «route», «netstat», «ipfw», «ipfilter», «ipchain», «iptables» снимают текущую сетевую конфигурацию компьютера.
- Утилиты «netstat», «nmap» снимают информацию о текущих сетевых соединениях и открытых портах.
- Утилиты «Task manager», «pslist», «ps», «top» дают список текущих процессов – исполняемых программ.
- Утилиты «lsof» дают список открытых в текущий момент файлов.
- Утилиты «w», «last» дают список пользователей, вошедших в систему.
- Утилиты «date», «nlsinfo» дают информацию о текущем системном времени.

- Утилиты «ethereal», «tcpdump» дают возможность снять текущий сетевой трафик компьютера.
- Утилиты «lsmod», «kldstat» показывают список загруженных модулей ядра.

Какую именно короткоживущую информацию собирать и в каком порядке? Зависит от характера доказательств, которые мы предполагаем найти.

Когда речь идет о «взломе» исследуемого компьютера или заражении его вредоносной программой, следует собирать: содержимое ОЗУ, список процессов, список открытых портов, список пользователей, сетевую конфигурацию, образец трафика.

Когда дело касается электронной переписки или незаконного контента, возможно хранящегося на исследуемом компьютере, следует собирать: список процессов, информацию о криптодисках*, текущее время, возможно, сетевую конфигурацию.

Когда речь идёт о неправомерном доступе, предположительно осуществленном с исследуемого компьютера, следует собирать: список процессов, информацию о текущих сетевых соединениях, образец трафика.

По делам о нарушении авторских прав следует собирать: список процессов, текущее время, содержимое временных файлов и области подкачки*.

Вообще-то, если есть возможность, лучше собирать всю доступную короткоживущую информацию.

Порядок сбора информации рекомендуется такой, чтобы сначала собрать самую короткоживущую. А именно – собирать ее в такой последовательности:

- текущие сетевые соединения;
- текущие пользовательские сессии;
- содержимое ОЗУ;
- список процессов;
- открытые файлы;
- образец трафика;
- ключи и пароли;
- сетевая конфигурация;
- текущее время.

Когда сетевые моменты не важны (например, компьютер не подключен к сети в текущий момент), содержимое ОЗУ (дамп памяти) следует снимать в первую очередь – для его наименьшего искажения, поскольку, как уже указывалось, запуск любой программы изменяет состояние оперативной памяти ЭВМ.

Прежде чем снимать короткоживущую информацию с включенного компьютера, бывает необходимо преодолеть препятствия в виде:

- активного скринсейвера* (заставки) с парольной (парольно-биометрической) защитой;
- недостаточных привилегий текущего пользователя;
- заблокированных, отключенных или отсутствующих возможностей для подключения внешних устройств (порт USB, CD-привод).

Имеет ли право специалист задействовать для преодоления такой защиты специальные средства – программы, относящиеся к средствам несанкционированного доступа, вредоносным программам или средствам обхода защиты авторских прав?

Вообще-то имеет. Кроме вредоносных программ, использование которых противозаконно в любом случае.

Как выключать?

Каким способом следует выключать компьютер, который подлежит изъятию и который застали во включенном состоянии?

По большому счету, выбор сводится к двум вариантам: воспользоваться штатной командой выключения или выключить прерыванием электропитания. Рассмотрим преимущества и недостатки каждого из методов.

Команда завершения работы и выключения компьютера имеется в составе почти всех ОС. Часто та же команда не только завершает работу ОС, но и выключает электропитание. Иногда только завершает работу, а блок питания надо будет выключить вручную.

Во время процедуры завершения работы закрываются все открытые файлы, стираются временные файлы, иногда очищается область подкачки* (своп). Кроме того, всем текущим процессам посылается сигнал завершения работы. Что именно будет делать программа, получив такой сигнал, в общем случае сказать нельзя. Большинство программ просто завершают работу. Некоторые сохраняют промежуточные варианты данных. Другие, напротив, стирают свои временные файлы. Ряд вредоносных программ, таких как троян* или руткит*, могут при сигнале завершения работы целенаправленно уничтожить следы своего присутствия.

Если перед выключением специалист снял короткоживущие данные, как это описано выше, то почти все недостатки этого метода выключения можно считать компенсированными.

Кроме того, при завершении работы может сработать специально установленная логическая бомба*, которая уничтожит самые важные данные. Такие бомбы (к тому же связанные с командой завершения работы) встречаются редко, но все же...

Прерывание электропитания осуществляется вытаскиванием электрического шнура из компьютера. Причем лучше вытаскивать тот конец,

который подключен к компьютеру, а не тот, который к стенной розетке. Дело в том, что между розеткой и компьютером может оказаться источник бесперебойного питания*. Он не только станет поддерживать напряжение, но и может дать компьютеру команду завершения работы. Для ноутбуков, кроме того, следует извлечь аккумулятор.

В случае прерывания электропитания все временные файлы остаются нетронутыми. Но зато может быть нарушена целостность файловой системы, если прерывание электропитания застанет компьютер в момент проведения файловой операции. Испорченная файловая система в большинстве случаев может быть потом восстановлена, но не все экспертные системы поддерживают такую операцию, а экспертное изучение испорченной файловой системы затруднено. Кроме того, могут появиться локальные дефекты в некоторых открытых на запись файлах, например лог-файлах.

Вариант выключения выбирает специалист, исходя из обстоятельств дела: насколько важны временные файлы, можно ли предполагать наличие вредоносных программ. При отсутствии специалиста или при неясности указанных обстоятельств следует избрать метод выключения прерыванием электропитания.

Стоит ли упоминать, что примененный метод выключения компьютера должен быть указан в протоколе?

Некоторые криминологи даже советуют поступать следующим образом [52]. Если подозреваемый, в доме или на рабочем месте которого производится обыск, настаивает на «правильном» выключении компьютера, то согласиться для виду, но не позволять ему проделывать такую операцию. Вместо этого попросить написать или нарисовать необходимую последовательность действий. Этот документ приобщить к делу, а компьютер выключить методом обесточивания. При последующей экспертизе, если эксперт установит, что описанная подозреваемым последовательность действий должна была привести к уничтожению существенной для дела информации, это будет лишним доказательством вины и, возможно, отягчающим обстоятельством.

Автор относится скептически к такому совету и полагает, что применить его вряд ли удастся. Тем не менее следует помнить о возможности подобного обмана со стороны подозреваемого.

Например, многие модели криптодисков* имеют штатную возможность под названием «пароль для работы под контролем». Это альтернативный пароль, при вводе которого вместо подключения криптодиска безвозвратно уничтожается ключ шифрования[1], так что все защищенные

[1] Ключ шифрования не совпадает с паролем. Обычно пароль или производный от него ключ используется для зашифровки основного ключа шифрования. Таким образом, при уничтожении основного ключа пароль остается бесполезным, а данные - недоступными.

данные становятся недоступны навек. При этом либо имитируется внешний сбой, либо вместо истинного криптодиска подключается имитационный, с безобидными данными. Еще раз напомним, что «работа под контролем» – это не кустарная поделка, а штатная возможность всякой добротно сделанной системы защиты.

Работа с потерпевшими

Компьютерная информация имеет свойство легко и быстро утрачиваться. Задержка при сборе доказательств может привести к их неполучению. Поэтому потерпевших и свидетелей надо опросить на предмет таких доказательств как можно быстрее, не дожидаясь официального допроса.

У потерпевших и очевидцев следует узнать следующее.

Преступления, связанные с электронной почтой:

- адреса электронной почты – корреспондента и его собственный;
- сохранилось ли сообщение электронной почты (письмо), где именно оно сохранено;
- если сообщение сохранено, попросите передать его так, чтобы были доступны ВСЕ служебные заголовки, как это сделать, зависит от используемой программы-клиента;
- какая программа-клиент использовалась либо какой веб-интерфейс[1].

Преступления, связанные с веб-сайтами:

- каков адрес (URL) веб-сайта;
- услугами какого интернет-провайдера пользуется потерпевший;
- в какое время (желательно точнее) он посещал веб-сайт;
- сохранилась ли у него копия или скриншот* этого веб-сайта.

Преступления, связанные с телеконференциями (newsgroups):

- услугами какого интернет-провайдера пользуется потерпевший;
- каково имя телеконференции;
- через какой ньюс-сервер осуществлялся доступ к телеконференциям;
- какое использовалось ПО для доступа к телеконференциям, не осуществлялся ли этот доступ через веб-гейт;
- каков subject и другие данные сообщения;
- сохранилось ли сообщение телеконференции, где именно оно сохранено;
- если сообщение сохранено, попросите передать его так, чтобы были доступны ВСЕ служебные заголовки, как это сделать, зависит от используемой программы-клиента.

[1] Некоторые пользователи никогда не работали с клиентами электронной почты, а использовали только лишь веб-интерфейс. Они могут не понимать разницы между ними или быть уверены, что не существует иного способа работать с электронной почтой, чем при помощи браузера.

Заключение к разделу 3

Хотя многие устройства, несущие компьютерную информацию, а также многие программы предназначены для обычных пользователей, проводить с ними следственные действия нужно всегда с участием специалиста. Пользоваться – это далеко не то же самое, что изымать или проводить осмотр, фиксировать доказательства. При простом пользовании электронным прибором или программой происходит неконтролируемое изменение данных. Такое скрытое изменение нисколько не вредит функциональности устройства, оно заранее предусмотрено производителем. Но для следственных действий любое неконтролируемое или неявное изменение компьютерной информации недопустимо. Не допустить его может только специалист.

Чтобы обеспечить упоминавшуюся цепочку доказательности (корректность и целостность от момента начала следственного действия до момента завершения экспертизы), требуется участие специалиста, знакомого с особенностями хранения и обработки данных соответствующими электронными устройствами или программами.

4. Заверение контента

Для доказывания многих преступлений и правонарушений необходимо доказать распространение или обнародование некоторой информации. Возбуждение межнациональной розни, клевета, пропаганда наркотиков, распространение порнографии, нарушение авторских прав — в состав этих и других преступлений входит такое действие, как распространение информации или произведения. Разумеется, в данной книге речь пойдет только о распространении через компьютерные сети, прежде всего Интернет.

Как доказать факт наличия определенной информации в сети в определенный период времени, а также ее общедоступность? Как установить лицо, разместившее информацию, и доказать этот факт?

Сложности в доказательстве таких фактов суть следующие:

- невозможно произвести непосредственный осмотр размещенной информации (произведения), поскольку видеть можно лишь изображение на экране, возникшее вследствие сложных и не контролируемых процессов передачи, и преобразования изначально размещенной информации;
- подавляющее большинство веб-страниц — динамические, их контент зависит от времени, местоположения пользователя, его браузера, ряда случайных факторов;
- доступ к информации в Сети производится через посредство множества технических средств, о большинстве из которых не известно ничего определенного;
- во многих случаях доступ производится в интерактивном режиме, то есть для получения информации требуется проявление инициативы со стороны пользователя;
- существует много способов ввести в заблуждение пользователя, просматривающего информацию, — относительно самого факта размещения информации, ее содержания, адреса, времени;
- размещенную информацию в ряде случаев довольно просто и быстро убрать либо она уничтожается сама с течением времени;
- Интернет рассматривается многими как некая область особенной свободы или экстерриториальная зона, поэтому там существует много средств и возможностей для анонимизации, сокрытия следов, круговой поруки;
- существующие процессуальные нормы рассчитаны были исключительно на офлайновые* документы и доказательства, в них редко учтены технические особенности компьютерных сетей.

Методы фиксации доказательств тем не менее существуют. Рассмотрим наиболее распространенные методы размещения информации в Сети и укажем для каждого из случаев его особенности и приемлемые методы фиксации.

Размещение на веб-сайте

В простейшем случае размещение на веб-сайте сводится к помещению файла в соответствующую директорию на сервере.

В более сложных случаях для размещения информации могут потребоваться также следующие действия:

- регистрация или приобретение доменного имени*, настройка DNS-серверов* для него;
- установка и запуск веб-сервера*;
- приобретение услуги провайдера по организации и поддержанию веб-сервера (хостинг* или колокация*);
- настройка веб-сервера;
- создание или модификация исходного кода* веб-страницы на языке HTML, PHP и др.;
- создание или модификация CGI-скриптов* для поддержания работы веб-сайта;
- создание или заказ художественного оформления (дизайна) веб-сайта;
- настройка аутентификации и авторизации на веб-сайте;
- сообщение каким-либо способом адреса (URL) размещенного файла или соответствующей веб-страницы заинтересованным лицам, рекламирование такого адреса;
- отслеживание работы веб-сайта, его статистики посещений, трафика, количества скачиваний размещенной информации, отзывов посетителей и т.д.;
- обновление, актуализация размещенной информации;
- удаление или блокирование размещенной информации.

Каждое из указанных действий оставляет «цифровые» следы. Чем больше таких действий совершал злоумышленник, тем легче его идентифицировать и впоследствии доказать его вину.

Как видно, следы могут быть достаточно многочисленными. Впрочем, в данной главе речь идет не о поиске и изобличении лица, разместившего информацию, а о доказательстве наличия в Сети самой этой информации.

Практика

В российской практике применялись следующие способы удостоверения содержимого веб-сайта для судебных целей:

- распечатка веб-страниц через браузер*;
- распечатка + рапорт сотрудника милиции;
- осмотр веб-сайта следователем с понятыми;
- такой же осмотр, но с участием специалиста;
- ответ оператора связи (провайдера) на запрос о содержимом сайта;
- экспертиза;
- нотариальное удостоверение (осмотр сайта нотариусом).

Каждый из способов небезупречен. Хотя браузер и вся система WWW ориентированы на неподготовленных лиц, все же специальные знания требуются для того, чтобы убедиться в отсутствии ошибок и намеренных фальсификаций. Поэтому без участия специалиста корректность результата не гарантирована. Применение же экспертизы вроде бы избавляет от возможных ошибок. Но вызывает сомнение тот факт, что объект экспертизы (веб-страница, веб-сервер) находится не в распоряжении эксперта, а довольно далеко от него.

Просмотр

Цепочка преобразования информации на пути ее от сервера к пользователю дается следующей схемой:

информация на диске сервера – веб-сервер – браузер – изображение на экране

Разумеется, информация при прохождении указанной цепочки претерпевает значительные изменения. Они касаются не только ее формы представления, но и содержания. Преобразования формы в этой цепочке настолько многочисленны и многовариантны, что описать их все не представляется возможным. Постараемся упомянуть хотя бы те преобразования, которые затрагивают содержание информации.

Динамические веб-страницы

В самом начале эры WWW, в первой половине 1990-х, веб-страница была эквивалентна файлу на диске веб-сервера. То есть, например, при запросе пользователем веб-страницы «`http://example.com/folder/page.html`» сервер, расположенный по адресу «`example.com`», брал с локального диска из директории «`folder`» файл «`page.html`» и отправлял его содержимое пользователю, лишь добавив в начало служебный заголовок. Такие HTML-страницы называются статическими.

Затем появились динамические веб-страницы. По запросу пользователя веб-сервер не просто берет определенный файл, а исполняет более сложную последовательность действий. Из файла или группы файлов или

из базы данных веб-сервер выбирает не просто HTML-код, а программу. Затем эта программа исполняется, а результат ее исполнения отображается браузером пользователя. Причем исполнение программы может производиться: (а) веб-сервером или одним из его модулей; (б) внешней программой на стороне веб-сервера; (в) браузером пользователя или одним из его модулей; (г) внешней программой на стороне пользователя. Понятно, что вид динамической веб-страницы будет зависеть от многих факторов, в том числе от конфигурации ПО на стороне пользователя. В настоящее время практически все веб-страницы в Интернете – динамические.

Особенности браузера

Следует принимать во внимание, что передаваемый от веб-сервера к браузеру код (HTML-код с различными включениями) не воспринимается человеком непосредственно. Этот код – лишь набор команд браузеру по генерации изображения, которое уже воспринимается человеком, а следовательно, может вызывать какие-либо правовые последствия. Хотя HTML и другие используемые на веб-страницах языки стандартизованы [30, 72], один и тот же код может интерпретироваться по-разному в разных условиях. Отличия в интерпретации (представлении) одного и того же кода разными браузерами, как правило, невелики. Некоторые мелочи и нюансы в стандартах не описаны. Некоторые браузеры немного отклоняются от стандартов или имеют собственные расширения к стандартизованному формату. Все это не может привести к принципиальным отличиям во внешнем виде страницы.

Но есть моменты, которые могут привести к принципиальным, то есть содержательным отличиям. Это прежде всего включенные в HTML-код программы на других языках или объекты, отображаемые другими, внешними приложениями. Получив в составе веб-страницы такой объект, браузер пытается найти и загрузить модуль либо внешнее приложение для выполнения такого кода и отображения результатов. Такие внешние (по отношению к браузеру) модули и приложения значительно менее стандартизированы и могут показывать пользователю существенно отличающиеся изображения или не показывать ничего, если соответствующего модуля или внешнего приложения не нашлось.

Поэтому, фиксируя вид веб-страницы, следует установить, каким именно браузером формируется это изображение и отметить в протоколе версию браузера. Еще более важно установить, только ли браузер формирует изображение на экране, участвуют ли в этом иные модули или внешние программы, а если участвуют, то какие именно.

Адресация

Кроме изменений, связанных с передачей размещенной информации от сервера к пользователю, следует также упомянуть о возможных проблемах, связанных с адресацией.

Утверждение «В Интернете по такому-то адресу (URL) размещена такая-то информация» не всегда четко и однозначно задает место размещения этой информации.

В URL [28], как правило, используется доменное имя*. Оно является средством адресации. Распространено мнение, что каждому доменному имени соответствует определенный IP-адрес. Браузер получает доменное имя, затем при помощи DNS* разрешает его в IP-адрес и обращается к сайту по этому IP-адресу. Это верно лишь в первом приближении. На самом деле адресация эта, во-первых, не статична, а во-вторых, не всегда однозначна. Кроме того, пользователь может быть перенаправлен на иной веб-сервер в зависимости от разных обстоятельств. Для иллюстрации приведем два примера.

В первом примере показывается динамическое разрешение доменного имени в IP-адрес, так называемый механизм «Round robin DNS». При разрешении доменного имени «cnn.com» на несколько сделанных подряд запросов возвращаются восемь различных IP-адресов, причем в разной последовательности:

```
fnn@home$>host cnn.com
cnn.com has address 64.236.16.20
cnn.com has address 64.236.16.52
cnn.com has address 64.236.16.84
cnn.com has address 64.236.16.116
cnn.com has address 64.236.24.12
cnn.com has address 64.236.24.20
cnn.com has address 64.236.24.28
cnn.com has address 64.236.29.120
cnn.com mail is handled by 10 atlmail3.turner.com
cnn.com mail is handled by 10 atlmail5.turner.com
cnn.com mail is handled by 20 nycmail2.turner.com
cnn.com mail is handled by 30 nycmail1.turner.com
fnn@home$>host cnn.com
cnn.com has address 64.236.29.120
cnn.com has address 64.236.16.20
cnn.com has address 64.236.16.52
cnn.com has address 64.236.16.84
cnn.com has address 64.236.16.116
cnn.com has address 64.236.24.12
cnn.com has address 64.236.24.20
cnn.com has address 64.236.24.28
cnn.com mail is handled by 10 atlmail5.turner.com
cnn.com mail is handled by 20 nycmail2.turner.com
cnn.com mail is handled by 30 nycmail1.turner.com
```

```
cnn.com mail is handled by 10 atlmail3.turner.com
fnn@home$>host cnn.com
cnn.com has address 64.236.24.28
cnn.com has address 64.236.29.120
cnn.com has address 64.236.16.20
cnn.com has address 64.236.16.52
cnn.com has address 64.236.16.84
cnn.com has address 64.236.16.116
cnn.com has address 64.236.24.12
cnn.com has address 64.236.24.20
cnn.com mail is handled by 10 atlmail3.turner.com
cnn.com mail is handled by 10 atlmail5.turner.com
cnn.com mail is handled by 20 nycmail2.turner.com
cnn.com mail is handled by 30 nycmail1.turner.com
```

Веб-сайт cnn.com обслуживается сразу несколькими серверами. При разрешении доменного имени DNS-сервер выдает сразу восемь различных IP-адресов. Браузер может выбрать любой из них, но обычно выбирается первый. Выдавая IP-адреса в разном порядке, DNS-сервер пытается равномерно распределить нагрузку на эти сервера.

В данном случае все сервера, обслуживающие веб-сайт, имеют одинаковый контент* (информационное наполнение). Но могли бы иметь разный.

Второй пример показывает зависимость видимой веб-страницы от IP-адреса пользователя. Автор запросил одну и ту же веб-страницу «www.google.com» с двух различных компьютеров. У первого из них IP-адрес зарегистрирован за российским провайдером, у второго – за немецким. Ответы веб-сервера были различными.

```
-bash-2.05b$ lynx -noredir -source www.google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-
8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://www.google.ru/">here</A>.
</BODY></HTML>


fnn@home$>lynx -noredir -source www.google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-
8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF= "http://www.google.de/">here</A>.
</BODY></HTML>
```


При совершенно одинаковом запросе в первом случае пользователь был перенаправлен на веб-сайт «www.google.ru», во втором случае – на веб-сайт «www.google.de». Содержимое этих сайтов существенно различается. И не только языком.

Понятно, что контент* одного и того же веб-сайта (на взгляд одного и того же пользователя) может зависеть от времени суток, от просматривающего сайт пользователя, от некоторых случайных факторов.

Размещение в телеконференции (newsgroup)

Телеконференции* представляют собой систему серверов, объединенных между собой протоколом NNTP [53] и содержащих примерно один и тот же контент. Контент представляет собой множество сообщений (обычно коротких), организованных в группы с иерархической структурой имен [54]. Сообщения – короткоживущие, каждое из них, появившись на любом из серверов, за короткое время (минуты) распространяется по всем остальным, а через несколько дней устаревает и автоматически удаляется. Пользователь может подключиться по тому же протоколу NNTP к любому из серверов и получить с него все или только интересующие группы и отдельные сообщения, а также опубликовать свое сообщение.

Ньюсридер. Слева расположен список групп (телеконференций), на которые подписан пользователь, справа вверху – список доступных сообщений в выбранной телеконференции, справа внизу – выбранное сообщение

Вследствие особенностей используемого протокола, система телеконференций дает относительную анонимность пользователя. Возможно, из-за этого в телеконференциях присутствует значительное количество незаконного и сомнительного контента* – порнографии, контрафактной музыки. Правда, «тяжелый» контент для телеконференций неудобен. Например, фотография объемом 20-50 кбайт вполне помещается в одно сообщение. Музыкальное произведение в формате MP3 объемом 4-5 Мбайт должно быть разделено на несколько сообщений. Чем больше сообщений, тем труднее потом «читателю» собрать вместе исходный файл. Поэтому произведения большого объема, порядка десятков мегабайт и свыше, в телеконференциях не публикуются.

Из служебных заголовков сообщения телеконференции можно установить, через какой сервер этой системы (они обычно именуются ньюс-серверами или NNTP-серверами) сообщение было опубликовано. IP-адрес пользователя, опубликовавшего сообщение, в заголовках обычно не фиксируется. Системы аутентификации и авторизации в протоколе NNTP не предусмотрено, только ограничения на основании IP-адреса. Логи, в которых фиксируется, какой пользователь какое сообщение прочитал или опубликовал, серверами ведутся, но далеко не всегда. А когда ведутся, их объем редко позволяет хранить историю более чем за несколько суток.

Ниже приведен пример исходного кода сообщения в телеконференцию со всеми служебными заголовками (часть строк в середине пропущена).

```
Path:
newsfeed.rtcomm.ru!newsfeed.gamma.ru!Gamma.RU!newscon06.news.prodigy.net!pro
digy.net!border1.nntp.dca.giganews.com!nntp.giganews.com!nx01.iad01.new-
shosting.com!newshosting.com!post01.iad01!news.usenethost.com!not-for-mail
From: «B-Girl» <wacu28jd@msn.com>
Newsgroups: alt.bainaries.pictures.lolita.fucking
Subject: I filmed myself and want to find another sexy young girl to have
sex fun 00000029.jpg
X-Priority: 3
X-MSMail-Priority: Normal
Date: Thu, 14 Dec 2006 05:19:27
Lines: 848
Message-ID: <457fdd83$0$29368$5ec1c3@news.usenethost.com>
Organization: usenethost
X-Complaints-To: abuse@removethis-usenethost.com
Xref: newsfeed.rtcomm.ru alt.bainaries.pictures.lolita.fucking:21155

begin 664 47100000029.jpg
M_]C_X``02D9)1@`!`0```0`!``#_VP!#``,"`@,"`@,#`P,$`P,$!0@%!00$
M!0H'!P8(#`H,#`L*"PL-#A(0#0X1#@L+$!80$1,4%145#`\7&!84&!(4%13_
MVP!#`0,$!`4$!0D%!0D4#0L-%!04%!04%!04%!04%!04%!04%!04%!04%!04
M%!04%!04%!04%!04%!04%!04%!3_P``1"`'@`H`#`2(``A$!`Q$!_\0`
M'0```04!`0$!`````````````!`(#!08'`0`("?_$`%`0``$#`P,"!0("!P0&
...
```



```
MRK&J]"L%#5AP#)9#<'[JK):,'ZXT>-V@0-L'AE[.`X55T^EF9TSOC]7TYP#\
AK7>I])9I6A/HR/,<TW+CV6>BAF=25+:+U,=:[2@3/__9

end

http://www.USENETHOST.com 100% Uncensored, 100% Anonymous,  5$/month  Only!
```

Первый служебный заголовок «`Path`» указывает все ньюс-сервера, через которые это сообщение было передано (справа налево, разделенные восклицательным знаком). Видно, что публикация сообщения произведена через сервер **`news.usenethost.com`**, об этом же свидетельствуют заголовок «**`Message-ID`**» и подпись в последней строке сообщения. Никаких идентификационных данных пользователя не указано; правда, в поле «From» стоит адрес электронной почты, но это поле заполняется пользователем по собственному усмотрению и не проверяется.

В самом сообщении, как видно, кроме последней строчки с автоматической подписью содержится лишь изображение в формате JPEG, кодированное по алгоритму UUENCODE. В телеконференциях для кодирования бинарных данных (протокол NNTP умеет передавать только текст) применяются два алгоритма: «UUENCODE» и «yEnc» [W19]. Первый используется еще с 1970-х, второй введен относительно недавно, в 2001-м.

Для удостоверения наличия определенного контента в телеконференциях можно использовать один из способов, рекомендуемых в предыдущей главе «Размещение на веб-сайте», то есть провести осмотр, нотариальный осмотр или экспертизу. Для проведения осмотра или экспертизы придется подключиться к любому из ньюс-серверов, совсем не обязательно к тому же самому, на котором сообщение было впервые обнаружено. Их контент различается между собой лишь постольку, поскольку различается время хранения сообщений на разных серверах.

Бывают анонимные NNTP-сервера, владельцы которых утверждают, что не ведут логов, и этим стараются привлечь подписчиков.

Чтобы установить источник конкретного сообщения в телеконференцию, надо предпринять следующие действия:

- Получить само сообщение со всеми служебными заголовками. Эти заголовки обычно не показываются программой просмотра (ньюс-ридером*), чтобы их увидеть, надо специально включить соответствующий режим. Как это сделать, зависит от типа ньюс-ридера.
- По заголовкам установить, через какой сервер это сообщение было введено. Заголовок может быть и подложным, если источник предпринимал специальные меры для сохранения анонимности. Для надежности можно получить то же сообщение через несколько ньюс-серверов и сравнить их заголовки.
- Обратиться к администратору того сервера, через который сообщение

было опубликовано, и затребовать логи за соответствующий период. По ним можно установить IP-адрес, с которого сообщение опубликовано.

- Также можно поискать в телеконференциях другие сообщения, принадлежащие, судя по их содержимому, тому же источнику. Если первая попытка установить автора сообщения была неудачной, возможно, он попадется на следующем своем сообщении.

Когда источник установлен, следует изъять компьютер, с которого предположительно публиковалось сообщение в телеконференцию. Экспертиза может установить факт публикации, факт создания сообщения, факт наличия на этом компьютере того же контента, что и в сообщении.

Со стороны сервера факт публикации должен подтверждаться протоколом осмотра или экспертизы логов ньюс-сервера.

Также возможен перехват трафика. По протоколу NNTP сообщения передаются в незашифрованном виде. Экспертиза перехваченного трафика также будет доказательством размещения сообщения.

Если ожидается публикация сообщения в телеконференцию и при этом известен сервер, через который сообщение будет опубликовано, или же известна сеть, из которой оно придет, установить источник можно при помощи ОРМ «снятие информации с технических каналов связи», задействовав для этого СОРМ.

Сообщение в телеконференцию не является сообщением от человека к человеку, поскольку оно адресовано неопределенному кругу лиц. Следовательно, это сообщение не охватывается правом на *тайну связи* (ч. 2 ст. 23 Конституции). Поэтому для отслеживания сообщений лица в телеконференции и его NNTP-трафика не надо получать судебного решения.

Размещение в файлообменных сетях

Термином «файлообменные сети*» (также «пиринговые сети», «P2P-сети») называют семейство программ и протоколов, позволяющих создавать одноранговые[1] сети в пределах глобальной компьютерной сети для обмена файлами, а также сами эти сети. Целями создания и функционирования таких сетей являются надежность, независимость от какого бы то ни было центра, относительная анонимность, возможность функционирования на персональных компьютерах и «узких» каналах связи.

Файлообменные сети возникли в конце 1990-х как реакция сетевой общественности на репрессии по поводу распространения в Интернете контрафактного и иного незаконного и неэтичного контента. Его распространение через веб- и FTP-сервера легко отслеживается, распространители наказываются, а сервера закрываются.

[1] Одноранговой называется сеть без выделенных узлов, то есть сеть из равноправных участников (узлов), которые взаимодействуют друг с другом на одинаковых основаниях. Каждый узел в таких сетях выполняет функции как клиента, так и сервера.

При распространении файлов через одноранговые пиринговые сети отключение любого числа узлов не влияет на работоспособность сети в целом.

Наиболее известные файлообменные сети:

- Napster – одна из первых файлообменных сетей, ныне не работающая; имела единый центр, из-за чего была закрыта по иску правообладателей;
- eDonkey2000 (сокращенно ed2k) – крупнейшая гибридная файлообменная сеть; поиск выполняют специализированные серверы, связанные между собой; клиенты самостоятельно обмениваются файлами по протоколу MFTP;
- Overnet, Kad – децентрализованные технологии на базе протокола Kademlia, обслуживающие поиск по сети eDonkey (ed2k);
- Bittorrent – сеть, специализированная для распространения файлов большого объема;
- FastTrack, iMesh – первоначально была реализована в KaZaA;
- OpenFT – OpenFastTrack поддерживается клиентами giFT (KCeasy), mlDonkey;
- Gnutella – сеть, использующая протокол, разработанный компанией Nullsoft;
- Gnutella2 – сеть на расширенном протоколе Gnutella;
- Ares – файлообменная сеть для любых файлов с преобладанием музыкальных;
- Freenet, Entropy – анонимные сети;
- MP2P (Manolito P2P) – поддерживается клиентами Blubster, Piolet, RockItNet;
- NEOnet – файлообменная сеть, клиент – Morpheus;
- MUTE – клиенты: MFC Mute, Napshare;
- Nodezilla – анонимная файлообменная сеть.

Всего известно более 40 общедоступных пиринговых сетей.

Каждый желающий участвовать в файлообменной сети устанавливает на свой компьютер программу-клиент, одновременно являющуюся и сервером. Как правило, такие программы создаются энтузиастами и распространяются свободно. Для каждой из сетей существует по нескольку различных программ-клиентов под разные операционные системы. Некоторые клиенты поддерживают взаимодействие по нескольким протоколам одновременно.

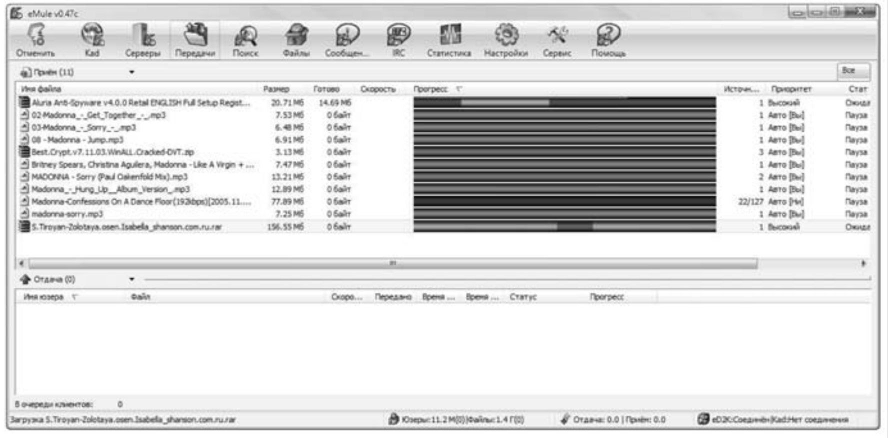
Клиентской программе достаточно соединиться с одним узлом файлообменной сети, чтобы получить возможность взаимодействовать с лю-

бым ее узлом. После подключения к Сети пользователь получает возможность скачивать к себе на компьютер любые имеющиеся в Сети файлы, а одновременно с этим другие пользователи получают возможность скачивать файлы, имеющиеся у него.

Наиболее известные программы-клиенты файлообменных сетей [W20] (в скобках указаны поддерживаемые сети/протоколы):

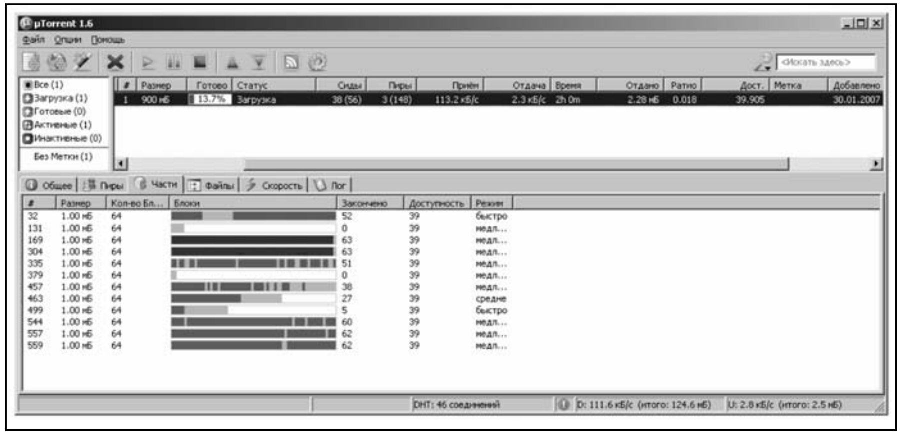
- aMule (eDonkey network, Kad network)
- eMule (eDonkey network, Kad network)
- Shareaza (BitTorrent, eDonkey, Gnutella, Gnutella2)
- FileScope (eDonkey network, Gnutella, Gnutella2, OpenNAP)
- MLDonkey (BitTorrent, Direct Connect, eDonkey network, FastTrack, Gnutella, Gnutella2, Kad Network, OpenNap, SoulSeek, HTTP/FTP)
- Napshare (Key network, MUTE network)
- giFT (eDonkey network, FastTrack, Gnutella)
- Gnucleus (Gnutella, Gnutella2)
- iMesh (FastTrack, eDonkey network, Gnutella, Gnutella2)
- KCeasy (Ares, FastTrack, Gnutella, OpenFT)
- Kiwi Alpha (Gnutella, Gnutella2)
- Morpheus (NEO Network, Gnutella, Gnutella2, BitTorrent)
- Zultrax (Gnutella, ZEPP)

Хотя указанные сети могут оперировать любым контентом*, по понятным причинам, основным контентом в них является незаконный, а также полузаконный, оскорбительный, неэтичный и другой проблемный контент. Обычно распространяются музыкальные MP3-файлы, фильмы, фотографии, дистрибутивы программного обеспечения.



Интерфейс клиента файлообменной сети «e-Mule»

В таких сетях можно найти практически любые произведения, пользующиеся хотя бы минимальным спросом. В том числе самые свежие, только что выпущенные в прокат кинофильмы и музыкальные альбомы. Правообладатели и власти постоянно предпринимают как попытки воспрепятствовать распространению контрафактного контента через такие сети, так и попытки прекратить функционирование файлообменных сетей вообще. Результаты этих усилий пока невелики.



Интерфейс клиента файлообменной сети «Torrent»

Следует заметить, что наряду с описанными файлообменными сетями, ориентированными в основном на контрафактный контент, существуют и небольшие, зато сугубо «законопослушные» сети, действующие с благословения правообладателей. Они используют такие же или сходные технологии, но являются коммерческими проектами. Естественно, имеют встроенные механизмы контроля за авторскими правами на передаваемый контент. Среди таких новых пиринговых сетей можно назвать «YouSendIt», «MediaMax» и «Xunlei» [W21].

Доказательство наличия контента

Доказательством наличия определенного контента в файлообменной сети могут служить свидетельские показания или заключение эксперта.

Поскольку присоединиться к такой сети может любой желающий, а для обычного использования файлообменного ПО специальных знаний не требуется, то не должно возникнуть проблем с обеспечением доказательств наличия контента. Сложнее обстоит дело с выявлением источника этого контента.

Выявление источника

Прежде всего следует заметить, что, поскольку файлообменные сети децентрализованные, понятие «источник файла» в них достаточно условно. Пока какой-либо файл лежит на единственном узле такой сети, этот узел можно назвать источником. При этом информация о файле (индексная информация) распространяется по всей сети. Но каждый узел, который начинает закачку этого файла, сам в тот же момент становится его источником, неотличимым от первичного. По окончании полной закачки файла узел либо продолжает служить его источником, либо прекращает – в зависимости от решения пользователя. Понятно, что пользующийся спросом файл, только появившись в файлообменной сети, сразу же начинает закачиваться множеством узлов и приобретает в их лице множество источников.

Поэтому не имеет смысла говорить о первичном источнике какого-либо файла.

Можно говорить лишь о нахождении файла (фрагментов файла) на конкретном узле и его доступности другим.

Передача же файла происходит обычно напрямую между узлами. Тогда можно определить IP-адрес узла-источника. Другой информации об этом узле, как правило, получить не удается.

Некоторые файлообменные сети не позволяют легко определить источник файла. Любой узел в таких сетях может выступать посредником при передаче, скрывая истинный источник. Это посредничество – чисто техническая особенность, не зависящая от воли пользователя. Поэтому хотя узел с технической точки зрения является посредником, с юридической точки зрения его владелец или оператор посредником не является, не имеет прямого умысла на такое посредничество и даже косвенного умысла не всегда имеет.

Таким образом, в ряде случаев мы имеем возможность относительно просто определить IP-адрес узла файлообменной сети, являющегося источником определенного файла. В других случаях (с узлами-посредниками) определение источника сильно затруднено. Определить же первичный или оригинальный источник файла не представляется возможным.

Доказательство использования

Доказательством того факта, что известное лицо использовало файлообменные сети, может служить следующее:

- протокол экспертизы компьютера интересующего нас лица, содержащий вывод о том, что на исследуемом компьютере было установлено ПО файлообменных сетей и это ПО использовалось по назначению;

- показания иного участника файлообменной сети о том, что он взаимодействовал в этой сети с узлом, имеющим тот же IP-адрес, что использовался интересующим нас лицом;
- протокол экспертизы компьютера иного участника файлообменной сети, содержащий вывод о том, что на исследуемом компьютере было установлено ПО файлообменных сетей, это ПО использовалось по назначению и обнаружены следы взаимодействия с IP-адресом интересующего нас лица;
- протокол осмотра или экспертизы компьютера оператора связи (провайдера), где зафиксировано наличие логов, отражающих информацию о трафике IP-адреса интересующего нас лица, причем в этом трафике присутствовали характерные для файлообменных сетей особенности (протоколы, порты, IP-адреса популярных узлов).

Следует упомянуть, что трафик файлообменных сетей не является тайной связи (ч. 2 ст. 23 Конституции), поскольку не относится к общению между человеком и человеком. Следовательно, для ознакомления с ним не требуется судебного решения. Однако такой трафик является тайной частной жизни (ч. 1 ст. 23 Конституции).

Виды преступлений

Некоторые считают файлообменные сети принципиально криминальными, поскольку легальный контент в них встречается редко, а основной трафик составляет в той или иной степени нелегальный. Утверждают, что именно ради такого контента файлообменные сети созданы и только ради него существуют.

Такая точка зрения не является общепринятой. Оппоненты возражают, что нелегального контента там не так уж много, а созданы файлообменные сети не только ради безнаказанности. Они имеют существенные преимущества перед другими способами распространения файлов, а именно, возможность быстро распространять большие объемы информации одновременно многим пользователям при использовании слабых и ненадежных каналов связи при периодической недоступности многих узлов.

Как бы то ни было, действующие на сегодня файлообменные сети сами по себе не поставлены под запрет ни в одной стране. Преследуются только правонарушения, совершаемые с их использованием.

Основными преступлениями, связанными с этими сетями, являются: нарушение авторских прав и распространение порнографии.

Контент и доменное имя

Правовая защита домена

Система доменных имен была придумана для облегчения запоминания человеком сетевых адресов. С массовым развитием системы WWW и с коммерциализацией Интернета доменное имя приобрело коммерческую ценность. А ценности нуждаются в законодательной защите. Тем более что стоимость самых дорогих доменных имен может исчисляться миллионами долларов. И законодательная защита была дана. Ныне домен – не просто удобная для человека форма сетевой адресации, но объект интеллектуальной собственности.

В одних странах отношения по поводу доменных имен сети Интернет напрямую регулируются законодательством, в других странах домены охраняются в числе прочих средств индивидуализации. В России доменное имя упоминается в законе «О товарных знаках...». В проекте части 4 Гражданского кодекса (вступает в силу с 2008 года) сначала присутствовала целая глава о доменных именах, но она была исключена при втором чтении. Тем не менее упоминание доменных имен как объекта регулирования осталось.

Путаница сайта и ДИ

Часто отождествляют веб-сайт и доменное имя, под которым этот сайт живет. На самом деле веб-сайт и домен – разные сущности как с технической, так и с правовой точки зрения.

Описанная путаница – следствие не только слабого понимания технических вопросов функционирования веб-сайтов. Неверному пониманию и отождествлению доменного имени и веб-сайта способствуют некоторые юристы, представляющие истцов по гражданским делам, связанным с веб-сайтами и информацией на них.

Как известно, обязанность найти ответчика лежит на истце. Его следует не просто найти, а представить суду доказательства того, что веб-сайт принадлежит ему. Веб-сайты не подлежат обязательной регистрации, нет никакой системы учета сайтов и их владельцев. А провайдеры (операторы связи) весьма неохотно сообщают данные о своих клиентах, ссылаясь на коммерческую тайну или защиту персональных данных.

В противоположность этому владельца доменного имени 2-го уровня узнать легко. Сведения о нем содержатся в общедоступной базе данных регистраторов доменных имен. Получить письменную справку с такими сведениями также несложно – распечатку с публичными данными сервиса whois легко заверит любой регистратор.

Таким образом, обстоятельства диктуют представителям истцов решение – назначить ответчиком не владельца веб-сайта, а владельца соответствующего домена.

Надо признать, что в большинстве случаев владелец домена 2-го уровня и владелец живущего на этом домене веб-сайта – одно и то же лицо. В большинстве случаев, но далеко не всегда. Кроме того, большинство веб-сайтов живут на домене не 2-го уровня, а 3-го. То есть на домене вида «www.example.com». Несмотря на то, что «www» – это стандартное имя 3-го уровня для веб-сайта, владельцы «www.example.com» и «example.com» могут быть разными.

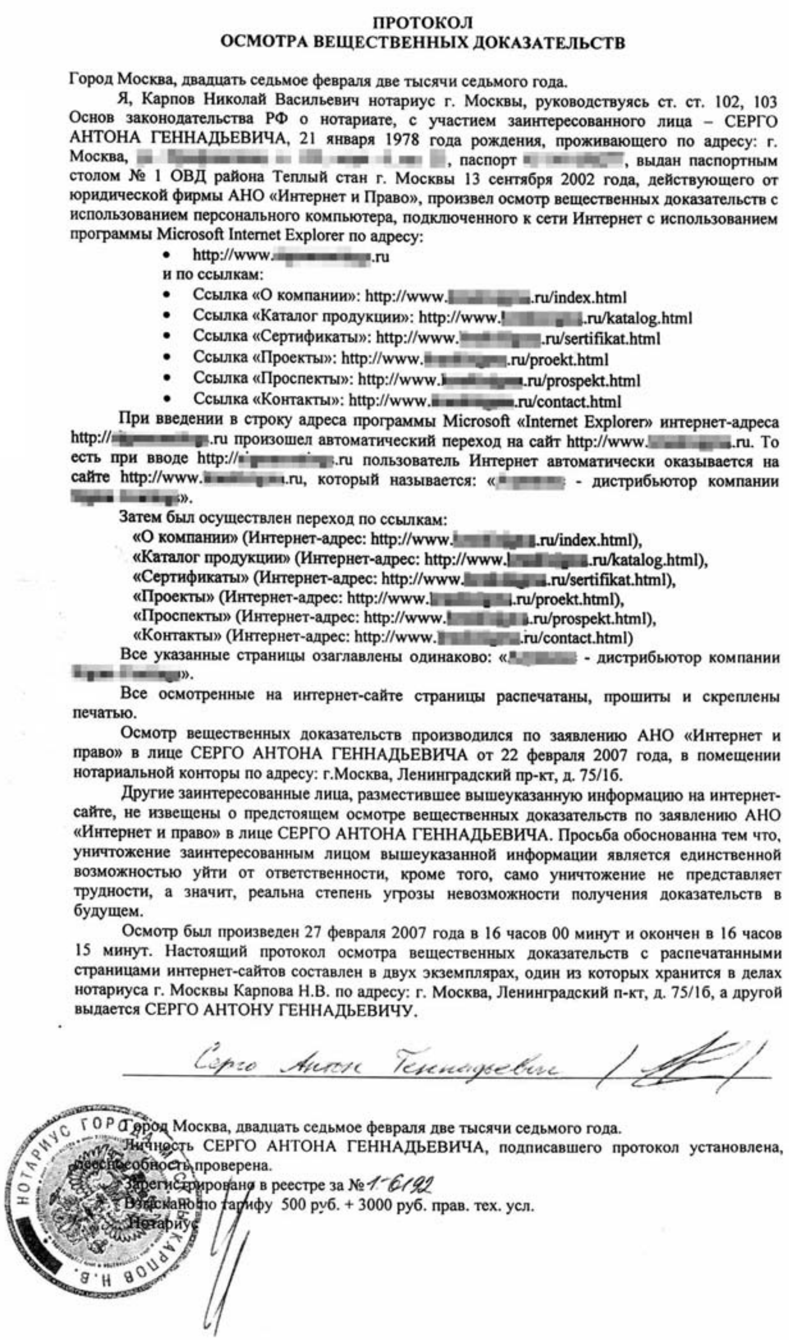
Также далеко не всегда совпадают владелец веб-сайта и владелец размещенного на этом сайте контента*.

Для гражданских дел можно попытаться возложить ответственность за контент сайта на владельца этого сайта, на оператора связи или даже на владельца доменного имени. За то, что создали условия размещения, не воспрепятствовали и т.д. В ряде случаев такое возложение ответственности истцам удавалось. Но для уголовных дел подобная натяжка не пройдет. Ответственность может нести только лицо, разместившее информацию на веб-сайте. В отношении владельца сайта, его провайдера, владельца домена можно говорить лишь о соучастии, и то – в весьма редких случаях.

Примеры

Ниже приводится образец нотариального протокола осмотра веб-сайта. Как указывалось ранее, нотариус не в состоянии обеспечить полную достоверность при фиксации содержимого (контента) веб-сайта. Нотариус не проверяет правильность разрешения доменного имени, не может противостоять различным способам подмены контента, не контролирует актуальность содержимого (отсутствие кэширования), не проверяет, отличается ли контент, отдаваемый пользователям из разных регионов, и так далее. Тем не менее достоверность такого осмотра – на достаточном уровне. Автору не известны случаи, чтобы суд отклонял такое доказательство по вышеуказанным мотивам.

Тем не менее, чтобы застраховаться от возможных ошибок или злонамеренных действий, в осмотре может участвовать и специалист. Ниже приводится образец протокола осмотра веб-сайта нотариусом совместно со специалистом.



ПРОТОКОЛ
ОСМОТРА ВЕЩЕСТВЕННЫХ ДОКАЗАТЕЛЬСТВ

Город Москва, двадцать седьмое февраля две тысячи седьмого года.

Я, Карпов Николай Васильевич нотариус г. Москвы, руководствуясь ст. ст. 102, 103 Основ законодательства РФ о нотариате, с участием заинтересованного лица – СЕРГО АНТОНА ГЕННАДЬЕВИЧА, 21 января 1978 года рождения, проживающего по адресу: г. Москва, [redacted], паспорт [redacted], выдан паспортным столом № 1 ОВД района Теплый стан г. Москвы 13 сентября 2002 года, действующего от юридической фирмы АНО «Интернет и Право», произвел осмотр вещественных доказательств с использованием персонального компьютера, подключенного к сети Интернет с использованием программы Microsoft Internet Explorer по адресу:

- http://www.[redacted].ru

и по ссылкам:

- Ссылка «О компании»: http://www.[redacted].ru/index.html
- Ссылка «Каталог продукции»: http://www.[redacted].ru/katalog.html
- Ссылка «Сертификаты»: http://www.[redacted].ru/sertifikat.html
- Ссылка «Проекты»: http://www.[redacted].ru/proekt.html
- Ссылка «Проспекты»: http://www.[redacted].ru/prospekt.html
- Ссылка «Контакты»: http://www.[redacted].ru/contact.html

При введении в строку адреса программы Microsoft «Internet Explorer» интернет-адреса http://[redacted].ru произошел автоматический переход на сайт http://www.[redacted].ru. То есть при вводе http://[redacted].ru пользователь Интернет автоматически оказывается на сайте http://www.[redacted].ru, который называется: «[redacted] - дистрибьютор компании [redacted]».

Затем был осуществлен переход по ссылкам:

«О компании» (Интернет-адрес: http://www.[redacted].ru/index.html),
«Каталог продукции» (Интернет-адрес: http://www.[redacted].ru/katalog.html),
«Сертификаты» (Интернет-адрес: http://www.[redacted].ru/sertifikat.html),
«Проекты» (Интернет-адрес: http://www.[redacted].ru/proekt.html),
«Проспекты» (Интернет-адрес: http://www.[redacted].ru/prospekt.html),
«Контакты» (Интернет-адрес: http://www.[redacted].ru/contact.html)

Все указанные страницы озаглавлены одинаково: «[redacted] - дистрибьютор компании [redacted]».

Все осмотренные на интернет-сайте страницы распечатаны, прошиты и скреплены печатью.

Осмотр вещественных доказательств производился по заявлению АНО «Интернет и право» в лице СЕРГО АНТОНА ГЕННАДЬЕВИЧА от 22 февраля 2007 года, в помещении нотариальной конторы по адресу: г.Москва, Ленинградский пр-кт, д. 75/1б.

Другие заинтересованные лица, разместившее вышеуказанную информацию на интернет-сайте, не извещены о предстоящем осмотре вещественных доказательств по заявлению АНО «Интернет и право» в лице СЕРГО АНТОНА ГЕННАДЬЕВИЧА. Просьба обоснованна тем что, уничтожение заинтересованным лицом вышеуказанной информации является единственной возможностью уйти от ответственности, кроме того, само уничтожение не представляет трудности, а значит, реальна степень угрозы невозможности получения доказательств в будущем.

Осмотр был произведен 27 февраля 2007 года в 16 часов 00 минут и окончен в 16 часов 15 минут. Настоящий протокол осмотра вещественных доказательств с распечатанными страницами интернет-сайтов составлен в двух экземплярах, один из которых хранится в делах нотариуса г. Москвы Карпова Н.В. по адресу: г. Москва, Ленинградский п-кт, д. 75/1б, а другой выдается СЕРГО АНТОНУ ГЕННАДЬЕВИЧУ.

Город Москва, двадцать седьмое февраля две тысячи седьмого года.

Личность СЕРГО АНТОНА ГЕННАДЬЕВИЧА, подписавшего протокол установлена, дееспособность проверена.

Зарегистрировано в реестре за № 1-6192

Взыскано по тарифу 500 руб. + 3000 руб. прав. тех. усл.

Нотариус

Заключение к разделу 4

Для доказательства факта размещения той или иной информации в Сети до сих пор не выработано единого подхода. Применяются различные методы: свидетельские показания, протоколы осмотра, нотариальные протоколы, заключения эксперта. Ни один из этих методов нельзя назвать безупречным. Главная трудность в том, что между размещенной информацией и глазами пользователя (нотариуса, эксперта) находятся многочисленные технические посредники. Проходя через них, данные претерпевают неоднократные преобразования, сложным образом маршрутизируются, переадресовываются, декодируются, представляются. В результате то изображение, которое предстает на экране компьютера, может относиться к оригинальной размещенной в сети информации весьма опосредованно. И к тому же варьироваться в зависимости от различных неконтролируемых пользователем факторов.

Поэтому на сегодняшний день задача заверения сетевого контента решается не вполне строго. Автор рекомендует компенсировать эту нестрогость дополнительными независимыми доказательствами, дополнительными источниками, просмотром из различных точек Сети, различными средствами. Иными словами, восполнять недостаток качества количеством.

5. Компьютерно-техническая экспертиза

Место и роль КТЭ

Общее

С точки зрения места в раскрытии и расследовании уголовного дела компьютерно-техническая экспертиза (КТЭ) ничем не отличается от других видов экспертиз.

Компьютерная информация, являющаяся объектом или средством совершения компьютерного преступления, хотя и может быть предназначена для обычных людей, но исследовать ее могут только специалисты. Практически любое обращение с компьютерной информацией требует специальных знаний. А источником таких знаний, согласно закону, может быть только специалист или эксперт. Устанавливать факты, касающиеся компьютерной информации, можно только на основании экспертизы. Отсюда и особая роль КТЭ при расследовании.

Несведущим людям может показаться, что многие действия над компьютерной информацией не требуют специальных знаний. Действительно, современные компьютеры и ПО предназначены для широкого круга пользователей. И пользователи (в том числе малоквалифицированные) успешно выполняют на них обычные задачи, такие как редактирование текстов, отправка и получение электронной почты, создание и распечатка рисунков. Зачем же тут специальные знания?

Чтобы найти ответ, давайте немного вспомним историю развития вычислительной техники. В 1960-х годах для работы на ЭВМ следовало не просто иметь специальные знания, но и быть программистом. Затем были созданы программы для решения некоторых типовых задач, и навык программиста перестал быть обязательным. Но управление работой ЭВМ по-прежнему было недоступно для неспециалиста. В 1980-х годах появились первые персональные компьютеры, научиться работать с которыми мог обычный человек. Обучение тем не менее все же требовалось. И это ограничивало рынок сбыта персональных компьютеров. Но ПО стремительно развивалось. И одним из главных направлений его развития являлось обеспечение простого, наглядного и относительно привычного интерфейса для неквалифицированного пользователя. Ориентация на массового покупателя – залог успеха для коммерческого ПО. Некоторые современные ОС делают освоение персонального компьютера довольно простой задачей, поскольку сводят «многомерное» управление к выбору из списка действий, а вместо технических терминов оперируют менее

адекватными, но более привычными для простого человека аналогами: «документ» вместо «файл», «папка» вместо «каталог», «отправка сообщения» вместо «установление SMTP-сессии» и так далее. Многие операции автоматизированы за счет снижения функциональности. Многие другие операции просто скрыты от пользователя. Все это стало возможным благодаря развитию программного обеспечения. Биты в современных компьютерах точно такие же, как и 40 лет назад. И набор арифметическо-логических операций процессора мало изменился. Кажущаяся простота – это не более чем поднятие пользователя на более высокий уровень абстрагирования от технической реализации операций. Такое поднятие вовсе не означает понимания. Напротив, простота управления достигается за счет снижения понимания сути производимых действий.

Приведем простую аналогию. В начале XX века управление автомобилем было неразрывно связано с его техобслуживанием (довольно трудоемким) и починкой. В течение нескольких десятилетий вождение автомобиля оставалось профессией, которой положено было учиться. По мере развития техники автомобиль превратился в потребительский товар, доступный самому широкому кругу. Ездить на машине перестало означать ее обслуживать. У некоторых современных моделей даже не открывается капот, поскольку пользователю это не нужно. В автошколах уже перестали учить устройство двигателя. Нужны ли специальные знания для современного автолюбителя? Почти нет. А для проведения экспертизы автотехники?

Для пользования современным компьютером специальные знания действительно не требуются. Это происходит благодаря высокой степени отчуждения пользователя от технической реализации обработки информации. Между «верхним слоем», то есть графическим интерфейсом пользователя, и «нижним слоем», то есть битовыми массивами данных, лежит много промежуточных «слоев» из форматов, протоколов, драйверов, API, системных функций и прикладных программ. На каждом из них остаются следы. Каждый «слой» вносит свою лепту в изменение компьютерной информации, в образование цифровых следов. Для поиска и изучения этих следов специальные знания нужны. Из-за отчуждения пользователя от реализации бóльшая часть информации от него скрыта. Почти все процессы происходят не так, как они представляются пользователю.

Кто может быть экспертом?

Неоднократно автору приходилось сталкиваться с вопросами на эту тему. Причем вопросы задавали следователи. А у вас есть лицензия на производство экспертизы? А ваше предприятие имеет сертификат экспертного учреждения? А у вас есть допуск на ознакомление с материалами уголовных дел?

Ответы на все подобные вопросы содержатся в Уголовно-процессуальном кодексе. «Эксперт – лицо, обладающее специальными знаниями и назначенное в порядке, установленном настоящим Кодексом, для производства судебной экспертизы и дачи заключения» (ст. 57 УПК). Как видно из этого определения, в законе отсутствуют требования о наличии определенного образования, опыта работы, какой-либо сертификации или лицензировании. Это, конечно же, не означает, что экспертом может быть любой. Специальные знания необходимы, но их наличие определяется следователем самостоятельно. Если следователь признал какое-либо лицо экспертом, поручив ему проведение экспертизы, то подозреваемый или потерпевший может лишь заявить отвод эксперту (ст. 198 УПК) и не более.

Когда эксперт или экспертное учреждение являются государственными, то они руководствуются также законом «О государственной судебно-экспертной деятельности в Российской Федерации» (№73-ФЗ). В нем предусматривается аттестация экспертов из государственных экспертных учреждений.

На деятельность иных, то есть негосударственных экспертов и экспертных учреждений действие этого закона распространяется частично. Какого-либо лицензирования, обязательной сертификации или аттестации для негосударственных экспертов не предусмотрено.

Какое же учреждение является экспертным, а какое – нет? Кодекс говорит, что «экспертное учреждение – государственное судебно-экспертное или иное учреждение, которому поручено производство судебной экспертизы в порядке, установленном настоящим Кодексом» (ст. 5 УПК). То есть любое негосударственное учреждение, которому следователь или суд счел возможным поручить проведение экспертизы (поручить на законных основаниях, естественно), автоматически становится экспертным.

Ни в УПК, ни в упомянутом законе, не содержится никаких отдельных упоминаний компьютерно-технической экспертизы, поэтому КТЭ производится по общим принципам.

По традиционным видам судебной экспертизы авторитет государственных экспертных учреждений и квалификация их экспертов редко подвергаются сомнению. Но по новому, всего 5-7 лет назад возникшему виду экспертизы – КТЭ – эти экспертные учреждения либо вообще экспертиз не проводят, либо способны проводить лишь простейшие их виды. Причина известна. Специалисты в области ИТ (а тем более, квалифицированные) пока еще не подготавливаются в массовом порядке. Средняя рыночная зарплата такого специалиста намного превышает ставки, которые в состоянии предложить любое из бюджетных учреждений (а государственное экспертное учреждение, согласно закону, может финансироваться только из бюджета).

Таким образом, следователь может выбрать в качестве эксперта любое лицо, в чьей компетентности он уверен. Никаких обязательных «сертификатов эксперта», лицензий и допусков не требуется. Разумеется, для оценки квалификации кандидата следователь может навести справки об образовании, опыте работы в сфере ИТ, должности. Опыт является определяющей величиной.

Когда есть выбор, автор рекомендует отдавать предпочтение гражданскому эксперту. В государственных экспертных учреждениях системы МВД (ЭКЦ, ЭКУ, ЭКО) если и имеются штатные эксперты по КТЭ, то лишь низкой квалификации, как правило, «крепостные», то есть работающие там, чтобы избежать призыва в армию. Кроме того, нагрузка на штатных экспертов МВД никак не позволяет им затрачивать на экспертизу более двух дней (обычная норма две экспертизы в день), что автор полагает неприемлемо коротким сроком для полноценного исследования.

Проблемы с пониманием

Эксперт призван дать заключение (ч. 1 ст. 57 УПК), а специалист – разъяснить вопросы (ч. 1 ст. 58). То и другое подразумевает объяснение неспециалистам фактов и обстоятельств из области специальных знаний. Но всегда ли возможно такое объяснение?

Оно возможно лишь тогда, когда некий процесс непонятен без специальных знаний, но его следствия или выводы целиком лежат в знакомой области. Например, неспециалист может не понимать, что такое отпечатки пальцев и как их снимают. Но вывод – человек касался пальцами предмета – понятен любому. Неспециалист может совершенно не разбираться в авиационной технике. Но «причиной аварии явилась ошибка пилота» – это каждому понятно. Неспециалист не может себе вообразить, как работает транзистор. Но как пользоваться радиовзрывателем – здесь нажал, там взорвалось – это понятно.

В отрасли ИТ встречаются ситуации, когда не только механизм и процесс лежат в области специальных познаний, но там же находятся следствия и выводы. Поэтому бывает так, что специалист затрудняется объяснить простыми словами не только почему, но и что, собственно, произошло.

Например, возьмем такое злодеяние, как вмешательство в процесс показа рекламных баннеров*. Специалист вряд ли сможет разъяснить суду механизм подмены адреса баннерного сервера через DNS-записи. Но и следствия этого деяния – пользователи увидят на веб-страницах рекламу, помещенную туда помимо их желания и без прямой санкции владельца веб-страницы вместо другой рекламы, которая тоже была помещена туда

помимо желания пользователей и без прямой санкции владельца веб-страницы – все целиком находятся в виртуальном мире и не могут быть разъяснены без предварительного разъяснения всех сложных взаимоотношений между участниками информационного обмена.

Разъясняя вопросы, требующие специальных знаний, специалист фактически занимается переводом с одного языка на другой. Для этого он не только должен в совершенстве владеть обоими языками. Попытки перевести с технического на юридический часто наталкиваются на такое препятствие: в другом языке просто не существует соответствующего термина. Да что там термина! Соответствующего понятия не существует.

Например, нетрудно перевести с технического термин «провайдер». На юридическом это означает «оператор связи». А вот как перевести термин «доменное имя»? Это совершено новый объект, возникший в Сети и не имеющий аналогов в офлайне*. Средство индивидуализации? Нет, под определение не подпадает. Ресурс нумерации? Тоже нет, фактически не соответствует. Приходится обходиться без перевода и вводить этот термин в юридический оборот. Но как объяснить его значение неспециалисту, если даже специалист учился несколько лет, прежде чем полностью понял, что такое доменное имя?

Еще пример. В ходе процесса судья поставил перед специалистом вопрос: идентифицирует ли IP-адрес компьютер в сети Интернет однозначным образом? Специалист ответил утвердительно. Тот же вопрос был поставлен перед экспертом. Эксперт ответил отрицательно. Оба они были правы, о чем и согласились, поговорив между собой. Дело в том, что эксперт отвечал на вопрос «теоретически», имея в виду абстрактный компьютер и любой IP-адрес. Разумеется, любой IP-адрес однозначным идентификатором не является. Специалист же был ознакомлен с материалами дела и отвечал на вопрос применительно к конкретному компьютеру и конкретному адресу. Фигурировавший в деле IP-адрес идентифицировал компьютер обвиняемого однозначно, о чем специалист и сказал.

Итак, следует признать, что для области ИТ сформулированная в УПК задача специалиста и эксперта не всегда является выполнимой. Но выполнять ее надо. Как следствие, эксперты и специалисты иногда превышают свои полномочия и не только «разъясняют вопросы», но и делают выводы.

Приемлемые вопросы

Для следователя и оперуполномоченного важно представлять, что именно может компьютерно-техническая экспертиза (КТЭ) и чего она не может. Также важно уметь верно формулировать вопросы для экспертизы.

На памяти автора следователь ни разу не поставил вопросы для КТЭ корректно. Оно и неудивительно. Чтобы правильно сформулировать вопрос, нужно знать большую часть ответа. И разбираться в терминологии. А чтобы знать специальные термины, нужно представлять, что они означают. Короче, нужно самому обладать специальными знаниями в области ИТ.

Была издана работа, содержащая перечень возможных вопросов для КТЭ [42]. Формулировки всех вопросов там заранее выверены и должны быть понятны эксперту. Следователю оставалось лишь выбрать нужный. Разумеется, ни к чему хорошему это не привело. Раньше, не имея подобной подсказки, следователь формулировал вопросы некорректно. Это приводило к объяснению между ним и экспертом. В ходе разговора вопросы уточнялись, следователь переписывал свое постановление в соответствии с рекомендациями эксперта. А пользуясь шпаргалкой, но по-прежнему не понимая значения терминов, следователь попросту выбирает из списка не те вопросы. В результате вместо плодотворного диалога получается, что эксперт просто выполняет ненужную работу. А нужную – не выполняет.

Автор полагает, что для формулировки вопросов для КТЭ всегда следует привлекать специалиста. Это может быть специально приглашенный специалист. Это может быть неофициальная консультация. В крайнем случае, сам эксперт, которому предстоит проводить КТЭ, поможет следователю верно поставить вопросы.

Автор, не желая повторять чужих ошибок, не станет приводить здесь списка возможных вопросов для КТЭ. Вместо перечня вопросов автор предпочитает дать перечень решаемых экспертизой задач с необходимыми разъяснениями.

Поиск информации

Поиск на компьютерном носителе документов, изображений, сообщений и иной информации, относящейся к делу, в том числе в неявном (удаленном, скрытом, зашифрованном) виде.

Автор рекомендует не конкретизировать вид и содержание искомой информации. Эксперт вполне может самостоятельно решить, относится ли тот или иной текст, изображение или программа к делу. В ходе поиска информации эксперту приходится просматривать глазами тысячи текстов и изображений. Понятно, что невозможно распечатать и приложить к заключению их все – с тем, чтобы потом следователь решил, что из найденного относится к делу. Эксперт в любом случае вынужден проводить первичную селекцию и принимать решение, что именно из найденного приобщать. Вынужден в силу объемов информации. Типичный объем архива электронной почты среднего пользователя – мегабайты. Для более актив-

ного – сотни мегабайт. Это не поместится ни в одно заключение (протокол). Поэтому эксперта следует ознакомить с уголовным делом или хотя бы кратко изложить его фабулу в постановлении о назначении КТЭ. И запросить у него поиск «любой информации, относящейся к данному делу».

Следы

Поиск «цифровых» следов различного рода действий, совершаемых над компьютерной информацией. Вопрос лучше формулировать не про следы, а про действия. То есть вместо «имеются ли следы создания таких-то веб-страниц?» лучше поставить вопрос так: «создавались ли на исследуемом компьютере такие-то веб-страницы?».

Когда компьютер используется как средство доступа к информации, находящейся в ином месте, и когда доступ к информации осуществляется на этом компьютере – в обоих случаях остаются «цифровые» следы, следы в виде компьютерной информации. КТЭ может определить, когда, при каких условиях и каким образом осуществлялся доступ. Кто его осуществлял, КТЭ определить не может. Лишь в некоторых случаях эксперту удается обнаружить некоторые сведения о пользователе исследуемого компьютера.

Действия, которые оставляют следы на компьютере или на носителе информации, включают: доступ к информации, ее просмотр, ввод, изменение, удаление, любую другую обработку или хранение, а также удаленное управление этими процессами.

Программы

Анализ программ для ЭВМ на предмет их принадлежности к вредоносным, к средствам преодоления ТСЗАП, к инструментам для осуществления неправомерного доступа к компьютерной информации, к специальным техническим средствам, предназначенным для негласного получения информации. А также анализ функциональности программ, принципа действия, вероятного их источника, происхождения, автора.

Иногда необходимо более глубокое исследование программ. То есть исследование не просто их свойств и функциональности, а происхождения, особенностей взаимодействия с другими программами, процесса создания, сопоставление версий. Такое глубокое исследование подразумевает дизассемблирование программы, запуск под отладчиком (пошаговое исполнение), исследование структуры данных. Это предмет отдельной экспертизы, иногда ее называют программно-технической. Редко можно найти эксперта, сочетающего специальные знания по ИТ и по программированию. Поэтому рекомендуется проводить две отдельные экспертизы – первая изучает содержимое компьютерных носителей, а вторая особенности обнаруженных программ.

Такое более глубокое исследование программ необходимо далеко не всегда. Например, вредоносность программы – это совокупность ее функций [81, 70]. Вредоносность может установить эксперт-специалист по ИТ. А вот для сопоставления объектного* кода программы с фрагментом исходного* кода необходимо участие эксперта-программиста.

Время

Установление времени и последовательности совершения пользователем различных действий.

Благодаря наличию у компьютера внутренних энергонезависимых часов и простановке в различных местах временных меток становится возможным определить, когда и в какой последовательности пользователь производил различные действия.

Если внутренние часы компьютера были переведены вперед или назад (в том числе неоднократно), все равно имеются возможности восстановить правильное время и правильную последовательность событий. Перевод часов компьютера сам по себе оставляет следы. А если еще было и сетевое взаимодействие, то есть возможность сопоставить моменты событий, зафиксированные данным компьютером, с событиями по иным источникам и выяснить сдвиг внутренних часов.

Задача выполнима даже в том случае, если системный блок, содержащий внутренние часы, не находится в распоряжении экспертизы. Только по носителю информации (например, НЖМД*) можно получить кое-какие сведения о последовательности событий. Чем больше информации на носителе, тем полнее будет восстановлена картина.

Отмечена даже такая экзотическая задача, как подтверждение/опровержение алиби подозреваемого, который утверждает, что в определенное время работал за компьютером [43]. В этом случае, хотя речь не идет о компьютерном преступлении, для проверки алиби потребуется КТЭ.

Пользователь

Оценка квалификации и некоторых других особенностей личности пользователя исследуемого компьютера.

При достаточно интенсивном использовании компьютера человек неизбежно оставляет в нем «отпечаток» собственной личности. Документы, фотографии, музыка, переписка, настройки, оформление, закладки, временной режим работы, подбор программ – все это индивидуализирует информационное содержимое компьютера. Все это отражает интеллект пользователя, его эмоции, наклонности, способности.

Нет уверенности, что вопрос полностью лежит в сфере КТЭ. Возможно, ради более строгого подхода такая экспертиза должна быть комплексной, компьютерно-психологической. Во всяком случае, вопрос квалифи-

кации пользователя в области ИТ точно в компетенции эксперта, проводящего КТЭ. Конечно, для оценки квалификации на исследуемом носителе должны находиться соответствующие объекты, результаты интеллектуальной деятельности – написанные пользователем программы, переписка по нетривиальным техническим вопросам, сложные программные инструменты (например, отладчик).

Следует заметить, что некорректно ставить вопрос об «установлении личности пользователя компьютера». Любые выводы о личности на основе найденных на диске плодов интеллектуальной и творческой деятельности могут носить лишь предположительный характер.

Итоги

Итак, обычно перед экспертом, проводящим КТЭ, ставятся вопросы:

- о наличии на исследуемых объектах информации, относящейся к делу (в том числе в неявном, удаленном, скрытом или зашифрованном виде);
- о возможности (пригодности) использования исследуемых объектов для определенных целей (например, для доступа в сеть);
- о действиях, совершенных с использованием объектов, их времени и последовательности;
- об идентификации найденных электронных документов, программ для ЭВМ, о признаках пользователей компьютера;
- о свойствах программ для ЭВМ, в частности, о принадлежности их к вредоносным.

Неприемлемые вопросы

Контрафактность

Отдельного разъяснения требуют вопросы, связанные с контрафактностью экземпляра произведения, представленного в цифровой (электронной) форме. Недопустимо ставить перед экспертом вопрос, является ли исследуемый экземпляр произведения контрафактным. Контрафактность – это вопрос правоотношений между правообладателем и пользователем, но никак не вопрос состояния экземпляра. Один и тот же экземпляр может быть контрафактным и легальным (лицензионным), в зависимости от того, оплатил ли пользователь стоимость лицензии, истек ли ее срок, выполнены ли лицензионные условия и других обстоятельств. Иными словами, контрафактность – это юридический, а не технический факт. Устанавливать его эксперт не может [L02].

Конечно, эксперт может найти косвенные признаки контрафактности, то есть такие особенности, которые обычно (подчеркиваю – обычно!) встречаются на контрафактных экземплярах и обычно не встречаются на

лицензионных. Но прямыми доказательствами такие признаки не будут, поскольку контрафактный экземпляр легко превращается в лицензионный путем заключения договора с правообладателем или его представителем (а это сводится к уплате соответствующей суммы). И, напротив, лицензионная копия легко становится контрафактной при нарушении пользователем лицензионных условий. В обоих случаях сама копия при таких «превращениях» ни на бит не изменяется.

Перед экспертом следует ставить вопросы о наличии признаков контрафактности – любых или конкретных, которые заранее известны следователю.

Впрочем, среди юристов существует мнение, что никаких «признаков контрафактности» вообще не бывает. А признаки исполнения экземпляра произведения не должны подвергаться экспертизе, поскольку их наличие или отсутствие не связано с контрафактностью экземпляра. Согласно этой точке зрения, для доказательства нарушения авторских прав непременно следует установить изготовителя экземпляра произведения, доказать отсутствие у него разрешения от правообладателя и лишь затем проводить экспертизу изъятых экземпляров с целью установить, действительно ли они были изготовлены тем же способом, на том же оборудовании.

Предположим, в лапы правоохранительных органов попал компакт-диск с произведением. Диск имеет тип CD-R, записан с использованием ПК, обложка отпечатана на ксероксе, голограмма отсутствует. Следует ли устанавливать и закреплять с помощью экспертизы все перечисленные признаки? Обсуждаемая позиция утверждает, что нет, не следует. Поскольку отсутствует причинная связь между кустарным исполнением и отсутствием разрешения правообладателя. Следует доказывать нарушение авторских прав, что сводится к доказыванию отсутствия разрешения, то есть договора, между изготовителем (не продавцом!) диска и правообладателем, либо между изготовителем и уполномоченным представителем правообладателя, либо между изготовителем и обществом по коллективному управлению авторскими правами. А метод изготовления диска с фактом заключения такого договора никак не связан. Следовательно, признаки исполнения диска ничего не доказывают. Даже косвенно.

Впрочем, автор с изложенной позицией не согласен. И авторитеты (например, Верховный Суд) на этот счет еще не высказались.

Стоимость

Технический специалист не может определить ни стоимость программного продукта, ни ущерб правообладателю. Стоимость является предметом товароведческой или экономической экспертизы.

Ценообразование на программные продукты и цифровые фонограммы – это отдельная большая тема. Происходит оно несколько иначе, чем в отношении материальных товаров. При этом издержки производителя – далеко не самый важный фактор. Если в отношении материального товара цена на различных рынках для различных групп потребителей может отличаться и в 2, и в 3, и даже в 5 раз (больше – вряд ли), то в отношении «нематериального» программного обеспечения цена может различаться в бесконечное число раз даже в пределах одной страны. Нередки случаи, когда правообладатель передает право на использование программного продукта (лицензию) совершенно бесплатно для некоторых потребителей, а с других потребителей берет значительные суммы.

Например, в отношении золотого кольца цена в один доллар является однозначным указателем на криминальное происхождение. Покупатель не может не знать, что таких цен на такой товар не бывает. На рынке же программных продуктов встречаются вполне легальные и при этом добротные товары по цене в 1 и даже в 0 долларов. При этом их аналоги могут продаваться за сотни долларов. Поэтому покупатель не может быть уверен в контрафактности, ориентируясь на низкую цену. Даже подозрений на контрафактность может не возникнуть.

Правомерность доступа

Эксперт не может определить правомерность доступа, осуществлявшегося с исследуемого компьютера или на исследуемый компьютер. Правомерность – это, как и контрафактность, факт юридический, а не технический.

Но эксперт может определить ряд других фактов, которые позволят следствию и суду квалифицировать доступ как правомерный или неправомерный. Это следующие факты:

- к какой именно информации осуществлялся доступ (для последующего решения вопроса, является ли она охраняемой законом компьютерной информацией);
- предпринимал ли обладатель информации, к которой был осуществлен доступ, какие-либо меры для ее защиты и ограничения доступа (для решения вопроса о конфиденциальности этой информации);
- присутствует ли на электронном документе или носителе гриф «коммерческая тайна» (для решения вопроса об отнесении этой информации к коммерческой тайне [44]) или иной гриф;
- является ли данный способ доступа общепринятым способом для публичных сетевых ресурсов.

Нуждается в пояснениях последний пункт. Правомерность или неправомерность доступа определяется не только законами (каковых для Интернета не очень много) или договорами (каковые не могут быть заключены между всеми пользователями и владельцами ресурсов). Во многих

случаях правомерность определяется обычаями делового оборота (ст. 5 ГК). Например, порт 3389/tcp используется для удаленного управления компьютерами с ОС «Windows». Никаких публичных сервисов на этом порту ожидать нельзя. Поэтому попытки доступа на этот порт со стороны постороннего лица следует расценивать как неправомерные. Порт 80/tcp, напротив, в подавляющем большинстве случаев используется для публичного HTTP-сервиса. Поэтому пользователь, осуществляя попытку доступа к этому порту чужого сервера, может ожидать на нем наличия общедоступного веб-сайта. Такую попытку нельзя признать неправомерным доступом. Итак, одно и то же действие по отношению к различным портам должно квалифицироваться по-разному. При этом статус обоих упомянутых портов закреплен лишь в технических стандартах и в неписаных обычаях делового оборота сети Интернет.

Оценка содержания

Эксперт может найти на исследуемом компьютере (носителе) тексты и сообщения по определенной тематике, однако он не имеет права оценивать содержание этих текстов, их авторство.

Также эксперт не может действовать в качестве переводчика, если тексты на ином языке. Возможно, исключение составляет тот случай, когда в переписке используется жаргон или транслитерация. Хотя задача в этом случае вроде бы лингвистическая, но соответствующих специалистов среди обычных лингвистов нет. Это как раз тот случай, когда лучший переводчик – не переводчик, а специалист в предметной области. Для «перевода» текстов с жаргона или с нестандартного транслита можно назначить отдельную комплексную экспертизу – лингвистическо-компьютерную. А можно поручить эксперту в рамках КТЭ «преобразовать найденные тексты в доступную для восприятия форму без изменения их смыслового содержания, а также разъяснить используемые в текстах специальные термины и выражения».

Ниже для иллюстрации приводится реальный диалог по ICQ из одного уголовного дела. Автор специально выбрал пример попроще, с использованием кириллицы. В случае же применения собеседниками транслитерации, да к тому же транслитерации далеко не канонической, о подобный диалог читатель мог бы сломать глаза.

```
Слушай а ты не знаешь где можно Civilization2 скачать?(это игра)
ТЫ ЧЕ?! ДУРАК?!
СОВСЕМ ПОЕХАЛ ЧТОЛИ?!
ОНА ВЕСИТ ТО СКОЛЬКО?!
А мне пофигу! Я вчера на 56$ сосканил!
ВОТ НЕНАВИЖУ КОГДА ТАК ОТРУБАЮТ!!!!!!
КАК?
Прлсто взяли и отрубили! Я уж думал пароль кончился....
```

```
:) Да у меня тоже такое в последнее время бывает...
Слушай... Ты мне так и не сказал как по сети в кваку резаться.
Здорова!!!
Здарово!!!
Пришол чтоли?
Ну так...
Здесь тебе привет от ученицы!!!
От Сашки чтоли? :)))
Мы тут по порно лазием!!
:))))))))))))
Рульно!!!
Ты где ща лазаеш?
Дан!! Дай пасс.
У менямои на исходе, а в переди еще вся ноч!!!!
Я те патом по возможности отдам...
Я простог в последнее время обленился!!! :((((( :))))
Дан!! Не молчи!!
Ты меня слышышь?
Слушай UFO выйдииз инета побазарить надо!!!!!!!
Давай.... А ещё, кокой у тебя номер в Одиго?
А как тебя туда занесло??:-)))
А газета то МоСковсКая?
А может это ФсБля А-ааа...:-)))))))))))))))))))))))))
Не-а...
Ты на щёт чего??
Слишком длинный:-))))
Давай на кнт.ru
Чё за инфа???
Слушай где мне УРл короткий достать?
Ну типа как ты говорил www.haker.net
Чё хоть куриш та?
Дай хоть какой нибудь сайт прикольный:-)))
Нет...
avt393381
Нет ты мне дал avt239776...
Держи на два бакса
--------------------
avt202265
UTew8hNC
--------------------
Ладно пора спать, а то завтра хрен встану. Полтинник принесу в воскресение
Пока!!!!!
```

Неподготовленный человек вряд ли поймет, что речь идет о применении вредоносных программ и неправомерном доступе к компьютерной информации, а также о сбыте результатов такого доступа.

Резюме

Итак, в рамках КТЭ нельзя ставить следующие вопросы:

- о лицензионности/контрафактности экземпляров произведений, записанных на исследуемых носителях;

- о правомерности действий, произведенных с использованием исследуемых объектов;
- о стоимости компьютеров, носителей, прав (лицензий) на содержащиеся там программы;
- о переводах найденных текстов, интерфейсов программ, переписки и т.п. (кроме разъяснения терминов и жаргона).

Объекты исследования

Оригинал или копия?

Существует мнение, что на экспертизу следует представлять только оригинал носителя компьютерной информации – НЖМД, компакт-диск, флэш-накопитель и т.д. А исследовать его копию якобы неприемлемо.

Это мнение не основано на законе. Ни в УПК, ни в законе «О государственной судебно-экспертной деятельности в Российской Федерации» (№73-ФЗ) такого требования не содержится. Более того, содержится запрет повреждать объект исследования без особого разрешения следователя.

Автор полагает (и многие исследователи с этим согласны), что исследовать в ходе КТЭ оригинал носителя вообще нежелательно. Чтобы гарантировать неизменность информации, а также оставить возможность проведения повторной или дополнительной экспертизы, надо оставить оригинал нетронутым. А все исследования проводить с его копией. Это не только надежнее, но и удобнее, поскольку копию можно сделать на таком носителе, который лучше приспособлен для имеющихся у эксперта инструментов, надежнее, быстрее.

Это относится не только к изготовлению копии носителя в ходе КТЭ, но и к копированию носителя вместо его изъятия при проведении обыска или выемки.

Например, во время обыска специалист может изъять диск сервера целиком, а может на месте скопировать все его содержимое (естественно, на низком уровне, на уровне контроллера) на свой диск. Допустимо ли это с процессуальной точки зрения? Разумно ли с технической точки зрения?

Есть следующие аргументы:

1. Некоторые методы исследования носителя непременно требуют оригинала. Другие с равным успехом работают с копией. Во время изъятия может ли специалист предположить, какие вопросы поставят перед экспертом и какие методы он станет применять? По мнению автора, может. Тем более что методы, требующие непременно оригинала, используются крайне редко.

2. Возможны ошибки при копировании диска. Их возникновение ставит под угрозу проведение экспертизы вообще. Но насколько вероятны такие ошибки? Верификация после копирования носителя разве не решит проблему? По мнению автора, решит. Кроме того, специалист должен использовать для копирования лишь проверенные средства и методы, которые не только не допускают ошибок, но и детектируют внешние ошибки.

3. Достаточна ли компетентность специалиста, участвующего в следственном действии, проводящего копирование диска? По мнению автора, найти такого специалиста несложно.

4. Поймут ли понятые суть происходящих действий? Изъятие и опечатывание оригинала диска им, безусловно, понятно. А снятие копии? Смогут ли они уверенно утверждать, что именно проделывал специалист? По мнению автора, им этого понимать и не обязательно. На то и предусмотрен специалист, чтобы проводить действия, требующие специальных знаний.

5. Может ли произойти при копировании диска утрата некоторой информации? Например, заводской номер диска, число секторов. По мнению автора, утраты не произойдет, если копировать на уровне контроллера диска, а внешние признаки оригинала записать в протокол.

6. Если применять снятие копии вместо изъятия оригинала носителя, это позволит не прерывать (или прервать ненадолго) рабочий процесс у владельца носителя. Остановить работу сервера на несколько дней ради проведения экспертизы – за что потерпевшему или непричастному провайдеру такое наказание?

7. В некоторых случаях копирование носителя страхует от потери данных вследствие недолговечности оригинального носителя. Например, в случае КПК. Лучше на месте снять копию памяти, чем до экспертизы поддерживать КПК в заряженном состоянии (не нарушая целостность печатей). Или в случае старого диска, склонного «сыпаться», то есть постоянно увеличивать количество дефектных блоков.

Методы КТЭ

Исследование файловых систем

Чтобы носитель компьютерной информации мог содержать файлы, он должен быть размечен и отформатирован под определенную файловую систему*. Разметка* состоит в создании на носителе разделов* (партиций), внутри которых могут быть образованы логические диски (тома). Форматирование логического диска (тома) состоит в создании на нем пустой файловой системы. Некоторые виды носителей способны содержать единственный раздел (партицию), например, дискеты.

Файловая система – это структура для организации хранения информации в виде файлов и доступа к ней. Файл обязательно предусматривает заголовок и тело. В заголовке содержится имя файла, другие его атрибуты и указание на расположение тела файла. В теле файла записываются данные, то есть содержимое файла. Практически все файловые системы предусматривают древовидную структуру: файлы включаются в состав директорий* (каталогов), которые, в свою очередь, могут включаться в другие директории. Минимальная единица хранения определяется параметрами носителя (например, размером сектора НЖМД) и файловой системой; обычно она именуется блоком или кластером. Тело файла всегда занимает целое число таких блоков.

Наиболее распространенные файловые системы таковы.

Название	**Макс. емкость**	**Комментарии**
FAT12	16 Мб	Используется только на дискетах
FAT16	2 Гб; для Windows-NT и последующих: 4 Гб	Единственная ФС для MS-DOS и ее клонов. С момента создания поддерживается ОС Юникс. Ныне считается устаревшей для компьютеров, но широко используется на иных устройствах – MP3-плеерах, камерах, флэш-накопителях
FAT32	2 Тб	Оригинальная ФС для Windows-95-OSR2 и последующих, является модификацией FAT16. Применяется в некоторых мультимедийных носителях.
NTFS	16 Эб (1 Эб=2^{60}б)	Оригинальная ФС для Windows-NT и последующих. Поддерживает сжатие и шифрование данных, а также восстановление после сбоев
UFS	256 Тб–1 Йб (2^{80}б) (UNIXFile System)	Стандартная, или «родная», ФС для всех типов UNIX, а также MacOS-X. Существует несколько модификаций под различные клоны Юникс
Ext2fs	32 Тб	Оригинальная ФС для ОС Linux. Наследует свойства UFS. Предусматривает восстановление целостности после сбоев
Ext3fs	32 Тб	Развитие ФС Ext2fs. Добавлено журналирование транзакций для улучшения и ускорения восстановления после сбоев
Ext4	1 Эб (1 Эб=260б)	Дальнейшее развитие ФС Ext3. Уменьшена фрагментация и повышена производительность

ISO-9660 этой		Популярная ФС для компакт-дисков и DVD. Есть несколько модификаций ФС: Joliet, Rock-Ridge, ISO-13490 и др.
HPFS (High- то- File System)	64 Гб Performance	Оригинальная ФС для OS/2. Основана на принципах FAT с добавлением неко- рых свойств по ускорению доступа и оптимизации
HFS	MacOS-6 и 7 – 2 Гб MacOS-7.5 – 4 Гб; MacOS-7.5.2 и послед. – 2 Тб	Стандартная ФС для MacOS
HFS Plus	2 Тб	Дальнейшее развитие HFS
UDF (Universal Disk Format)		ФС для DVD и некоторых CD

С другими файловыми системами можно познакомиться в специальной литературе [W10, W11], всего их известно несколько десятков.

Как правило, каждая ОС имеет встроенную поддержку для одной или нескольких файловых систем. При помощи дополнительного ПО (драйверов) ОС может понимать и иные файловые системы.

Если работать с носителем (диском) помимо штатных функций для соответствующей файловой системы, то можно увидеть больше информации, чем доступно через файловую систему. Такая скрытая информация может быть обнаружена в четырех местах – свободных блоках, хвостах файлов, ADS и неиспользованных разделах.

Свободные блоки. При стирании файлов штатными средствами ОС блоки, содержащие тело файла, отмечаются как свободные, но сразу не перезаписываются. Запись в эти блоки может быть произведена позже, при последующих операциях. Таким образом, свободные блоки, если они хоть раз использовались, содержат фрагменты старых, удаленных или измененных файлов. Правда, не всегда можно восстановить первоначальную принадлежность и последовательность этих блоков.

Хвосты файлов. Как указывалось, тело файла должно занимать целое число блоков (кластеров) на носителе. Если файл короче, то остаток последнего блока, его хвост или «slack space» будет содержать прежнюю информацию, то есть фрагмент старого файла.

Alternate data streams (ADS) – это дополнительные тела для файла в файловой системе NTFS, которые могут содержать сопутствующую информацию. Они недоступны с помощью штатных средств ОС и поэтому представляют скрытую для пользователя информацию.

Свободные и специальные разделы. Неиспользуемые и неразмеченные части диска также содержат информацию, которая была там прежде.

Иногда можно наткнуться на целый бывший раздел. Есть также разделы специального назначения, например, для свопинга или для хранения содержимого криптодиска.

Кроме того, на некоторых типах носителей встречаются технологические, не предназначенные для пользователей области, например, Host Protected Area (HPA). При помощи соответствующих программ они все же могут быть использованы и порой используются для хранения скрытой информации.

Копирование носителей

Любые экспертные исследования носителей компьютерной информации надо проводить, не изменяя их содержимого, если только это возможно. А возможно это всегда.

Исключением можно считать те случаи, когда эксперт не обладает исследовательским оборудованием или носителем нужной емкости. Учитывая, что исследовательским оборудованием в данном случае является самый обычный компьютер, а хорошее экспертное ПО распространяется бесплатно, такие причины автор не склонен считать уважительными. Но на практике это встречается. Надо напомнить, что если при экспертизе содержимое исследуемого носителя изменяется, некоторая оригинальная информация с него уничтожается, то, согласно УПК, на это следует получить предварительное разрешение от следователя, назначившего экспертизу.

Все исследователи единодушно рекомендуют делать копию оригинального носителя и проводить исследования с ней, а оригинал сохранить в неизменности для контроля и возможной повторной/дополнительной экспертизы. Если на экспертизу поступила копия, то ее также следует оставить в неприкосновенности в качестве мастер-копии, а исследования проводить над снятой с нее рабочей копией.

Для обнаружения скрытой информации копировать носитель нужно не средствами ОС, то есть не на уровне файловой системы, а уровнем ниже. Копирование надо производить на уровне контроллера устройства (также используется термин «Bit stream copying/imaging»). При этом копируется как информация, содержащаяся в файловой системе, так и скрытая для нее – свободные блоки, хвосты файлов и т.д.

В принципе, возможны исследования носителей на еще более низком уровне – на физическом. Для НЖМД это означает, что считывание производится не встроенными в накопитель магнитными головками, под управлением встроенного контроллера, а некими внешними средствами. При этом возможно снять остаточную намагниченность или намагниченность на границах магнитных дорожек и таким образом восстановить даже те данные, которые были недоступны для штатных магнитных головок исследуемого НЖМД. Это позволяет восстановить перезаписанные

(в том числе перезаписанные неоднократно) данные. Но такая экспертиза требует специального очень дорогого оборудования. Ограничимся рассмотрением экспертных исследований на уровне файловой системы и на уровне контроллера устройства.

Итак, оригинальный носитель перед проведением экспертизы копируется. Можно скопировать его на другой (такого же размера или большего) аппаратный носитель, а можно создать образ носителя в специальном файле или разделе. Копирование «носитель на носитель» можно произвести как предназначенным для этого отдельным устройством (дупликатором дисков), так и с помощью компьютера, использовав соответствующее программное обеспечение, например, программу «dd». Копирование «носитель в файл» производится только программно, специальным ПО, например, программой «dd».

Копирование же на уровне файловой системы (также используется термин «logical copying/imaging/backup») применимо лишь в ограниченном числе случаев, например, при изучении только лог-файлов.

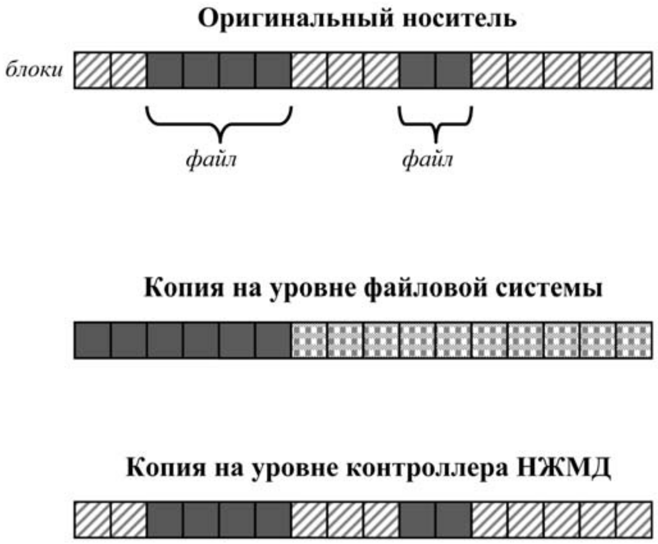


Схема копирования на уровне файловой системы (logical copying) и копирования на уровне контроллера диска (bit stream copying)

Копирование носителя может являться составной частью экспертизы. Копирование может быть проведено во время следственного действия вместо изъятия оригинального носителя. В последнем случае на экспертизу передается копия, но ее необходимо сохранить неизменной, так же как в случае с передачей на экспертизу оригинального носителя.

Есть опасение, что не все программные и аппаратные инструменты одинаково хорошо справляются с задачей копирования носителя.

Действительно, некоторые инструменты могут либо неточно/неполно копировать, так что содержимое копии отличается от оригинала, либо вносить какие-либо изменения в оригинал.

В Национальном институте юстиции США (National Institute of Justice, U.S. Department of Justice) были протестированы несколько таких программ [W12]. Согласно методике испытаний, корректность снятия копии содержимого (образа) диска определяется 4 параметрами:

- совпадение копии с оригиналом;
- возможность верификации копии;
- сохранение неизменности оригинала;
- детектирование внешних ошибок.

Проведенными исследованиями показана корректная работа следующих программ:

- dd из состава ОС FreeBSD 4.4 (без ошибок);
- Encase версии 3.20 (с тремя ошибками);
- Safeback версии 2.18 (с двумя ошибками);
- Safeback/DOS версии 2.0 (с четырьмя ошибками);
- dd из состава GNU fileutils 4.0.36, ОС Red Hat Linux 7.1 (без ошибок).

Разумеется, проводились и иные исследования в иных организациях, но автор приводит данный источник (National Institute of Justice) как наиболее авторитетный из известных. Использование упомянутых программ для снятия образа диска во время экспертизы или при проведении следственного действия не вызовет у специалистов сомнений по поводу корректности копирования.

Для сохранения неизменности оригинала или для дополнительной гарантии такой неизменности оригинальный носитель при копировании подключается в режиме «только чтение». Для этого во всех операционных системах, кроме Windows, используется режим «`ro`» команды монтирования файловой системы (`mount`). А для Windows, где такого режима не предусмотрено, используются специальные программные или аппаратные блокировщики записи, которых существует на рынке немало.

Для гарантии тождественности копии или образа диска после копирования следует произвести верификацию. В упомянутых выше программах и некоторых других предусмотрен режим верификации. Если его нет, то побитное сравнение содержимого оригинала и копии можно произвести иными программами.

Хэш-функции для удостоверения тождественности

В зарубежной практике для удостоверения целостности и неизменности данных на носителе используются однонаправленные хэш-функ-

ции*. Например, при снятии специалистом образа диска на месте происшествия подсчитывается хэш-функция, значение которой заносится в протокол. Эксперт, получив на исследование копию, подсчитывает с нее хэш-функцию. Если ее значение совпадает со значением, внесенным в протокол, эксперт и иные лица получают уверенность, что исследуемая копия совпадает с оригиналом с точностью до бита.

Аналогично хэш-функция используется для контроля целостности отдельных файлов. Например, при изъятии логов. Подсчитывается хэш-функция от лог-файла, она заносится в протокол. Если имеется уверенность в правильном подсчете хэш-функции, то сам лог-файл можно, в принципе, никак не оформлять, не опечатывать, а переписать на переносной носитель без формальностей. Значение хэш-функции в протоколе обеспечивает неизменность файла при копировании и последующем хранении. Совпадение значений хэш-функции гарантирует полное совпадение файлов [18].

Отметим, что все эти выкладки – чистая теория. В отечественной уголовной практике контроль целостности на основе хэш-функций не применяется (хотя в гражданских делах были прецеденты).

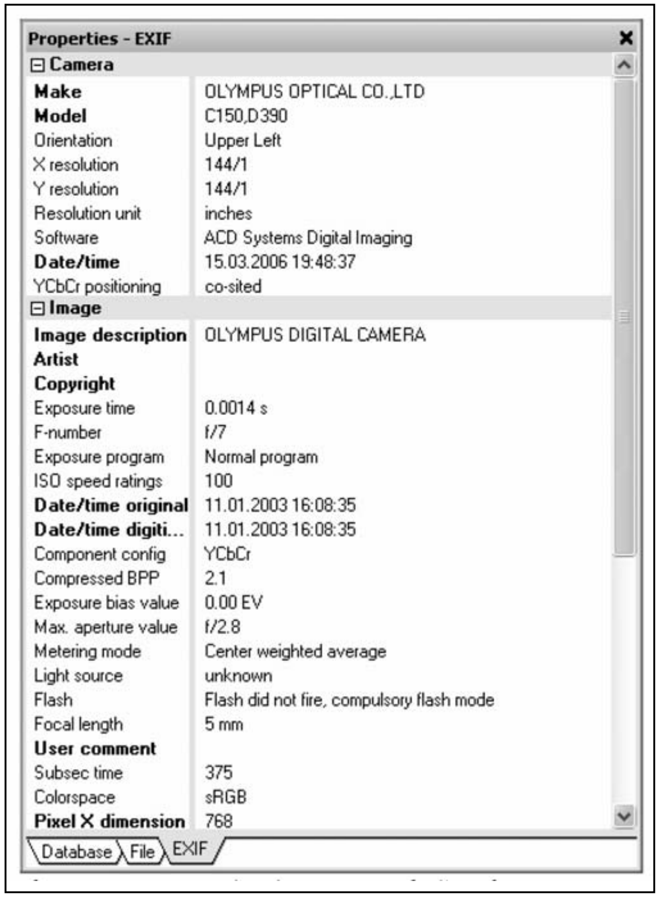
В качестве хэш-функций обычно используются широко известные алгоритмы MD5 [18, 33] и SHA-1 [34]. Они имеют достаточную стойкость. Хотя есть и гораздо более стойкие хэш-функции, например, SHA-256, SHA-512, WHIRLPOOL.

В России указанные алгоритмы имеют такую же стойкость, как и за рубежом, но они не являются стандартными. У нас имеется собственный стандарт для алгоритма хэш-функции – ГОСТ Р-34.11. Имеются даже его программные реализации, которые можно приспособить для вычисления хэш-функции от образа диска. Проблема в том, что хэш-функция считается криптографическим преобразованием, а его реализации – криптографической (шифровальной) техникой. Применение такой техники регламентируется соответствующими нормативными актами, она подлежит обязательной сертификации, использующие ее информационные системы – аттестации, а деятельность по обслуживанию шифровальной техники – лицензированию. Понятно, что при снятии копии диска специалистом в полевых условиях никак невозможно провести аттестацию системы и обеспечить соблюдение условий сертификата на шифровальную технику, даже если бы такой сертификат у специалиста имелся.

Поэтому автор не может рекомендовать официальное использование однонаправленных хэш-функций для удостоверения целостности информационного содержимого носителей. Их, конечно, полезно использовать. Можно даже заносить значение MD5 в протокол. Но нельзя ссылаться на совпадение значений хэшей в качестве доказательства неизменности данных.

Исследование файлов

Файлы, содержащие документы (текстовые, графические, табличные, комбинированные), очень часто несут кроме самого документа много служебной и сопровождающей информации, которая не видна для пользователя. Часто пользователь даже не подозревает о ее существовании. Однако эксперт о ней знает, а следовательно, может без труда извлечь такую дополнительную информацию из файла.



Служебная информация из необработанного файла формата JPEG позволяет получить дополнительные данные: модель фотоаппарата, время съемки, использование вспышки и многое другое

Например, в файлах с изображениями формата JPEG (jpg) хранятся сведения о прикладной программе или оборудовании, при помощи которой файл создавался или редактировался. В документах формата MS-Word хранится идентификатор (логин) создавшего пользователя, исходное размещение файла, прежние версии текста и много чего другого.

Шутка, обошедшая весь русский сегмент Интернета, – всего лишь полное имя файла, извлеченное из скрытых атрибутов документа MS-Word:

"C:\Хрень по работе\Гемор\Тупые клиенты\Неплательщики\охуевшие\Уважаемый Сергей Анатольевич.doc"

Как при исследовании отдельных файлов (кроме простейших текстовых или ASCII-файлов), так и при исследовании дисков, иных носителей, компьютеров имеет смысл поставить перед экспертом вопрос касательно обнаружения скрытой, служебной информации, предусмотренной соответствующим форматом файла.

Другие типы носителей

Флэш-накопители

Весьма распространенные носители компьютерной информации на основе флэш-памяти не только надежнее, но и значительно удобнее исследовать, сняв предварительно их копию. Разумеется, речь идет о копировании не на уровне файловой системы, а на уровне контроллера устройства, то есть bitstream-копировании. Также копию можно снимать не в ходе КТЭ, а при изъятии таких накопителей.

Проще всего сделать копию, подключив такое устройство к лабораторному компьютеру с ОС типа UNIX или Linux. В этих системах есть все необходимое для безопасного (без возможности записи) подключения и побитового копирования. При вставлении такого накопителя в USB-разъем или иное устройство чтения оно опознается операционной системой. Если опознания не произошло, значит, не хватает соответствующего драйвера (модуля ядра), который нужно доустановить.

Пример опознавания флэш-накопителя с интерфейсом USB:

```
# dmesg
umass1: PNY USB DISK 2.0, rev 1.10/0.50, addr 2
da4 at umass-sim1 bus 1 target 0 lun 0
da4: < USB DISK 2.0 1.09> Removable Direct Access SCSI-0 device
da4: 1.000MB/s transfers
da4: 124MB (253952 512 byte sectors: 64H 32S/T 124C)
```

Подключаем опознанный накопитель с опцией «ro» (только чтение):

```
# mount_msdosfs -o ro /dev/da4s1 /mnt/usbdrv/

# mount
/dev/ad6s1a on / (ufs, local)
devfs on /dev (devfs, local)
/dev/ad6s1e on /tmp (ufs, local, soft-updates)
```



```
/dev/ad6s1f on /usr (ufs, local, soft-updates)
/dev/ad6s1d on /var (ufs, local, soft-updates)
/dev/da4s1 on /mnt/usbdrv (msdosfs, local, read-only)
```

Чтобы исключить возможность изменения информации на устройстве, его подключение (монтирование) осуществляется с опцией «-r» (или «-o ro»), то есть в режиме read-only. Далее при помощи программы «dd» все содержимое устройства побитово копируется в файл, который и будет подвергнут дальнейшему исследованию.

```
# dd if=/dev/da4 of=/home/fnn/usbimage.bin conv=notrunc,noerror,sync
253952+0 records in
253952+0 records out
130023424 bytes transferred in 1271.039536 secs (102297 bytes/sec)
```

Получившийся у нас файл с образом накопителя `usbimage.bin` может быть подключен к экспертной программе – «EnCase» «FTK» или какой-либо другой.

Если копирование накопителя производится на месте, то будет полезно подсчитать контрольную сумму, а лучше – хэш-функцию полученного файла и занести ее в протокол. Значение хэш-функции, которая вычислена несертифицированным и неаттестованным криптографическим средством, официально не может служить доказательством неизменности файла. Однако ее совпадение со значением хэш-функции, которое вычислит эксперт, будет дополнительным способом убедиться в целостности данных.

```
# md5 usbimage.bin
MD5 (usbimage.bin) = 4d3de473b8c7f01ec6ed6888f61f8c43
```

После этого отмонтируем накопитель и извлекаем его из разъема.

```
# umount /mnt/usbdrv/

# dmesg
umass1: at uhub3 port 2 (addr 2) disconnected
(da4:umass-sim1:1:0:0): lost device
(da4:umass-sim1:1:0:0): removing device entry
umass1: detached
```

Подключение и копирование USB-устройства под ОС класса Windows представляется более проблематичным, поскольку отсутствует возможность подключения (монтирования) накопителей в режиме «только чтение». Все USB-устройства в этой ОС подключаются с возможностью чтения и записи, и ОС может производить запись на устройство без санкции со стороны пользователя и без его уведомления. Для накопителей с интерфейсами SCSI и IDE (ATA) выпускаются аппаратные блокираторы за-

писи, а для USB-устройств такого приспособления автору найти не удалось. Впрочем, некоторые модели флэш-накопителей имеют собственный аппаратный блокиратор записи в виде переключателя на корпусе.

Зашифрованные данные

Шифрование отдельных записей, файлов, разделов, дисков и трафика применяется злоумышленниками достаточно широко. Кроме того, функции шифрования встроены во многие виды программного обеспечения, где они задействуются автоматически. Эксперт должен быть готов ко встрече с зашифрованными данными, не должен считать такой случай безнадежным. Хотя современная сильная криптография считается практически непреодолимой, на практике оказывается, что во многих случаях добраться до зашифрованных данных можно [56].

Перечислим вкратце основные случаи, когда эксперт в состоянии расшифровать зашифрованные данные.

Использование слабой криптографии

То ли из-за недостатка знаний, то ли времени, но многие злоумышленники по сию пору продолжают использовать довольно примитивные шифры. Например, операция XOR (исключающее «или») с определенным байтом или короткой последовательностью байтов. Эта операция проще всего реализуется программно, и «на вид» такие данные выглядят зашифрованными. Но преодолеть XOR-шифрование очень просто. Иные виды слабой криптографии применяются редко, поскольку они не так просты, как операция XOR, а более стойкие алгоритмы шифрования доступны в виде исходного кода и библиотек.

Например, троянская программа «Back Orifice» использует XOR для шифрования своего трафика. Известные производители также были замечены в подобной халтуре: например, XOR с фиксированной последовательностью для шифрования паролей использовался в «Microsoft Office» до 2000 года, в «PalmOS» до версии 4 и в некоторых других программах.

Использование коротких ключей и паролей

Даже в случае применения сильной криптографии зашифрованные данные будут плохо защищены, если использован короткий пароль. Часто пароль служит ключом шифрования. В других случаях длина ключа или множество его значений искусственно ограничиваются. В подобных случаях эксперт может применить метод перебора, также называемый «brute force». Этот метод реализован во множестве программ для многих разных алгоритмов шифрования. На взгляд автора, всегда полезно погонять метод перебора в течение нескольких часов над зашифрованными данными; затраты рабочего времени незначительны, свободный ресурс процессора всегда имеется, а вдруг получится?

Не слабые, но намеренно ослабленные алгоритмы, такие как, например, 40-битный DES в экспортной версии «Windows-NT», также поддаются вскрытию методом перебора. Но для этого потребуется значительная вычислительная мощность – несколько компьютеров, объединенных в кластер. Для такой задачи имеется доступное программное обеспечение.

Использование словарных паролей

Вместо прямого перебора пароля или ключа («brute force») можно попробовать подобрать пароль по словарю. Большинство пользователей выбирают в качестве пароля осмысленное слово или фразу. Это позволяет резко сократить количество вариантов при переборе. Словарь всех распространенных языков содержит меньше миллиона слов. Вместе со всеми возможными комбинациями это всяко меньше, чем пространство неосмысленных паролей, то есть всех возможных сочетаний символов такой же длины. Несловарный пароль в 8 символов можно безуспешно подбирать месяцами. А такой же длины словарный пароль находится перебором за секунды.

В распоряжении эксперта есть как свободно распространяемые, так и проприетарные программы для подбора паролей по словарю, а также различные словари к ним.

В качестве дополнительного словаря автор рекомендует использовать все символьные строки, найденные на диске подозреваемого. Велика вероятность, что в качестве пароля он выбрал какое-либо слово, выражение, номер или иную строку символов, которую где-то видел или сам употреблял. В том и в другом случае эта строка может осесть на жестком диске в каком-либо виде.

Неаккуратное обращение с открытым текстом

При шифровании файлов и в некоторых иных случаях открытый текст зашифровывается, результат шифрования записывается на диск, а файл, содержащий исходный текст, удаляется. Если такое удаление произведено штатными средствами ОС, без использования специальной процедуры «затирания» содержимого файла, то открытый текст останется на диске и может быть восстановлен. То же относится к сообщениям электронной почты: при шифровании исходный текст удаляется из базы сообщений, но не затирается и может быть обнаружен, если поверх не запишутся иные данные. Во время редактирования файла, хранящегося на криптодиске, редактор может сохранять временные копии вне этого крипто-

диска, а операционная система может временно сбрасывать редактируемый текст или его части из ОЗУ в область подкачки*. Перед распечаткой на принтере незашифрованная копия данных записывается в очередь печати, то есть опять же на диск. Словом, пользователю трудно проконтролировать все файловые операции. При их проведении открытый текст часто остается на диске, где его можно потом найти.

Также копии открытого текста бывают разбросаны по оперативной памяти. Не все программы аккуратно обращаются с ОЗУ и затирают за собой содержимое памяти. Сняв дамп* ОЗУ в период активности шифрующей программы или после, можно найти в нем открытый текст.

Неаккуратное обращение с паролем

Как уже указывалось, словарный пароль легко подобрать. Зато неподбираемый пароль трудно запомнить. Тем более, трудно запомнить несколько длинных и неосмысленных паролей. Поэтому злоумышленник может записать пароли где-то – в файле, в записной книжке, в мобильном телефоне, на столе. Или использовать в качестве пароля уже имеющуюся вблизи рабочего места надпись, например, с наклейки на системном блоке.

Также подозреваемый может использовать один пароль для нескольких ресурсов разной степени защищенности. Это достаточно распространенная практика. Например, он сумел запомнить один длинный и неосмысленный пароль и использовал его для шифрования ключа к криптодиску и для доступа на веб-сайт. Из конфигурационного файла браузера эксперт извлекает все запомненные пароли и пробует применить их к криптодиску – вот и не сработала сильная криптография.

Нешифрованные имена файлов

Имена файлов при обработке записываются трудноконтролируемым образом в еще большее количество мест, чем содержимое (тело) файлов. В шифрованных архивах имена файлов часто не шифруются. Имена файлов часто запоминаются редакторами, файловыми оболочками. Даже если эксперту не удалось добраться до содержимого криптодиска, он наверняка найдет в нескольких местах на исследуемом компьютере оглавление этого криптодиска. По именам файлов многое можно сказать об их содержании. А если кроме имени известен еще и размер файла, то в отдельных случаях можно даже найти где-нибудь оригинал.

Известны случаи, когда расшифровать данные эксперту не удалось, но удалось получить оглавление зашифрованного диска. Соответствие имен файлов и их размеров известным файлам послужило доказательством. На таких доказательствах вполне может быть основано обвинение в нарушении авторских прав или в распространении порнографии.

Ректотермальный криптоанализ

Говорят, что человек – это слабейшее звено в системе информационной безопасности. Хотя автор и не согласен с рассмотрением человека в качестве «звена» или «элемента» информационной системы, следует признать, что большинство инцидентов происходят не из-за уязвимостей ПО или сбоев оборудования, а по вине персонала. Аналогичная ситуация наблюдается и в области исследования доказательств. Большинство известных автору случаев, когда эксперт смог расшифровать данные на исследуемом компьютере, – это сообщение пароля самим владельцем компьютера или оператором информационной системы.

Для того чтобы склонить подозреваемого или свидетеля к сотрудничеству со следствием, применяются различные методы, не входящие в сферу изучения криминалистики. Наука лишь отмечает, что человек является самым распространенным источником сведений для расшифровки зашифрованных данных.

Доступ к содержимому ОЗУ

В оперативной памяти могут храниться не только незашифрованные данные, но и ключи с паролями. Эксперт вряд ли получит доступ к работающему компьютеру с активированным криптодиском или иной системой шифрования, чтобы снять с него дамп оперативной памяти. Однако содержимое ОЗУ можно обнаружить в области подкачки, а также в дампах памяти, которые автоматически снимаются при сбоях в работе. Например, утилита «Dr.Watson» в Windows-2000 автоматически записывает дамп памяти сбойного процесса.

Содержимое ОЗУ с паролями, содержимое временных файлов и удаленных пользовательских файлов с паролями может быть найдено по всему диску в самых неожиданных местах. Систематический подход к задаче состоит в следующем. По исследуемому диску собираются все строковые величины, ключевые слова и фразы, они агрегируются и записываются в виде файла-словаря, который затем подключается к программе подбора паролей. Достаточно велика вероятность, что пароль хотя бы раз «осел» на диске или что пользователь использовал в качестве пароля слово или выражение, которое встречалось в прочитанных или написанных им текстах.

Использование кейлогера

В некоторых, достаточно редких случаях представляется возможность незаметно отследить действия подозреваемого, в том числе снять техническими средствами вводимый им пароль. Средства такие именуются кейлогерами (keylogger) и бывают программными и аппаратными.

Впрочем, этот метод относится, скорее, к ОРД, а не к экспертизе. Он более подробно описан в разделе 2.

Шифрование разделов и носителей

В некоторых носителях, таких как флэш-накопители, шифрование содержимого предусмотрено конструктивно.

По каким-то не вполне ясным для автора причинам некоторые проприетарные реализации такого шифрования на поверку оказываются нестойкими, уязвимыми, а то и вовсе притворными.

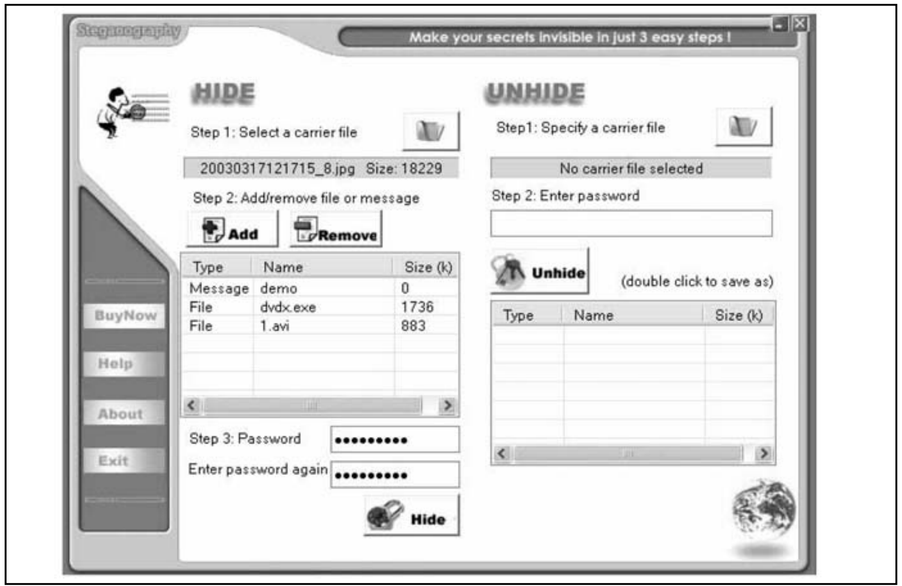
Поэтому, наткнувшись на проприетарную реализацию шифрования данных на носителе, эксперт должен первым делом предположить, что имеется намеренно или случайно оставленный производителем «черный ход». В ряде случаев такой ход обнаруживается простым поиском информации в Интернете. В других случаях производитель носителя сам берется расшифровать «надежно зашифрованные» данные (разумеется, по запросу правоохранительных органов, после исполнения ряда формальностей).

В отличие от проприетарных, открытые реализации шифрования все устойчивы. Во всяком случае, автору не известны случаи обнаружения в них «черного хода».

Стеганография

Этот метод, в отличие от шифрования, предусматривает сокрытие самого факта наличия информации на компьютере или в сообщении [66, 67].

Многие применяемые форматы данных (файлов и сообщений) содержат «нечувствительные» биты, которые могут быть изменены без ущерба



Одна из многочисленных программ для непрофессионалов, позволяющая скрывать произвольную информацию внутри файлов-контейнеров формата JPEG

для восприятия информации. Иные форматы предусматривают наличие обязательных, но неиспользуемых полей. И там и там может быть записана скрываемая информация.

Чаще всего в качестве стеганографических контейнеров используются изображения в формате BMP и JPEG, звуковые файлы в формате MP3 (MPEG-3), видеофайлы в формате AVI. Существует несколько программ (в том числе, свободных) для хранения информации в таких контейнерах и извлечения ее.

Стеганография чаще используется при пересылке сообщений. Для хранения же информации на компьютере применять стеганографические технологии неразумно, поскольку трудно скрыть наличие стеганографических программ. А если эксперт обнаружит такие программы, он непременно начнет искать скрытую информацию, то есть стеганография потеряет свое значение.

Ниже показан пример работы одного из инструментов для обнаружения стеганографических контейнеров – программы «`stegdetect/stegbreak`»:

```
$ stegdetect *.jpg
cold_dvd.jpg : outguess(old)(***) jphide(*)
dscf0001.jpg : negative
dscf0002.jpg : jsteg(***)
dscf0003.jpg : jphide(***)
[...]
$ stegbreak -tj dscf0002.jpg
Loaded 1 files...
dscf0002.jpg : jsteg(wonderland)
Processed 1 files, found 1 embeddings.
Time: 36 seconds: Cracks: 324123,   8915 c/s
```

Средства и инструменты

Экспертные инструменты и авторское право

Часто автору приходится слышать мнение, что все применяемые экспертом (специалистом) программные инструменты должны быть лицензионными*. В противном случае, дескать, результаты экспертизы или следственного действия считаются полученными с нарушением закона и недопустимыми.

На самом деле соответствующая норма (ст. 75 УПК) сформулирована так: «Доказательства, полученные с нарушением требований настоящего Кодекса, являются недопустимыми». То есть не имеют юридической силы лишь те доказательства, при получении которых нарушались требования УПК, а не какого-либо иного закона.

Нарушает ли эксперт требования УПК, используя нелицензированную копию программы? Не нарушает, ибо УПК (глава 27) не содержит каких-либо требований к инструментам эксперта.

Эксперт в своем заключении даже не обязан указывать, какие инструменты он использовал. Обязан указать лишь «примененные методики» (ст. 204 УПК). Методика – совсем не то же самое, что инструмент или программа. Почти все экспертные программы используют одни и те же методики исследования, а именно: доступ к носителю через функции файловой системы, доступ к носителю помимо файловой системы (через функции BIOS), контекстный поиск на носителе, детектирование форматов данных на основе сигнатур и так далее.

Нарушает ли эксперт законодательство об интеллектуальной собственности, используя нелицензированную копию программы? Оказывается, тоже нет. Статья 23 закона «Об авторском праве...» гласит: «Допускается без согласия автора и без выплаты авторского вознаграждения воспроизведение произведений для судебного производства в объеме, оправданном этой целью». В четвертой части ГК, которая с 2008 года приходит на смену закону «Об авторском праве...», эта норма сформулирована схожим образом: «Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение произведения для осуществления производства по делу об административном правонарушении, для производства дознания, предварительного следствия или осуществления судопроизводства в объеме, оправданном этой целью» (ст. 1278).

Программа для ЭВМ – это произведение. Инсталляция программы есть ее воспроизведение. Судебная компьютерно-техническая экспертиза – это как раз «для судебного производства» или «для производства предварительного следствия». Поэтому эксперт и специалист могут почти свободно использовать любой проприетарный софт, не опасаясь нареканий.

Многие компании-правообладатели и сами не возражают против бесплатного использования их программ экспертами или правоохранительными органами. Многие безвозмездно передавали образцы своего ПО для проведения экспертных исследований.

Таким образом, можно утверждать, что какие бы программы ни использовал эксперт в своих исследованиях, это само по себе не может служить основанием для непризнания результатов экспертизы.

Поиск информации на диске

Информация о файлах

Помимо самого файла, на диске сохраняется информация об этом файле в различных местах. Когда файл затерт, уничтожен без возможности восстановления, можно тем не менее установить и доказать факт его присутствия в прошлом по этим косвенным данным. Эти данные суть следующие:

- копии тела файла и их фрагменты в секторах диска, которые считаются свободными;
- заголовок файла в каталоге, а также во всех копиях этого каталога в свободных секторах диска;
- упоминания имени и, возможно, некоторых других атрибутов файла в «истории» и логах тех прикладных программ, которые его обрабатывали – редакторов, файл-менеджеров, клиентов электронной почты, архиваторов и т.п.;
- временные копии файла, которые создаются программами, которые этот файл редактируют или просматривают;
- промежуточные копии файла и его атрибутов, образующиеся при пересылке файла при помощи электронной почты, ICQ, FTP, веб-интерфейса;
- архивные копии диска, его отдельных каталогов, реестра, электронной почты и других объектов;
- миниатюры (thumbnails), которые создает ОС и некоторые вьюверы (программы просмотра) для ускорения просмотра списка файлов.

В некоторых случаях нет необходимости восстанавливать уничтоженную или зашифрованную информацию, достаточно лишь доказать ее наличие на исследуемом диске.

Например, по одному делу о нарушении авторских прав на программные продукты было установлено, что подозреваемый держал контрафактные копии программ на криптодиске*. Эксперт не смог подобрать ключ для расшифровки. Однако в этом и необходимости не было. Для подтверждения вины требовалось доказать не наличие программ на диске, а их использование подозреваемым. Эксперт обнаружил на диске многочисленные копии каталога криптодиска, записи в реестре, ярлыки (shortcuts) соответствующих программ, данные, обработанные этими программами, – и на этом основании сделал вывод, что программный продукт был установлен на исследуемом компьютере и использовался неоднократно.

В другом случае эксперт искал на диске подозреваемого электронные изображения денежных купюр, в подделке которых тот подозревался. Файлы с изображениями купюр оказались затерты без возможности восстановления. Однако сохранились миниатюры (thumbnails), которые автоматически создает ОС для показа списка файлов в каталоге. Для графических файлов миниатюра представляет собой уменьшенное изображение первой страницы. Несмотря на небольшой размер миниатюры, ее содержимое было видно достаточно четко. Эксперимент по созданию такой же миниатюры из большого изображения денежной купюры подтвердил гипотезу. Таким образом наличие файла с изображением на компьютере подозреваемого было доказано без обнаружения самого файла.

Подключение образа диска

Как указывалось выше, не обязательно изымать на экспертизу диск компьютера целиком. Вполне достаточно снять на месте bit stream-копию или образ этого диска. Исследуя этот образ, можно установить все, что и при исследовании самóго диска (исключение составляет особый вид экспертизы, крайне редко применяющийся в России). Но даже когда эксперту поступает сам магнитный диск, все исследования все равно проводятся над его образом, который снимается в самом начале экспертизы.

Образ диска может сниматься на такой же или большего объема диск по принципу «сектор в сектор». Другой, более удобный способ, когда образ диска создается в файле. В первом случае диск-образ физически подключается к лабораторному компьютеру и монтируется в режиме «read-only». Для этого используется команда «mount» с ключом «-r» или «-o ro»; такая команда есть в любой ОС, кроме «Windows». Для «Windows» придется подключать диск через специальное аппаратное устройство для блокировки записи. Во втором случае (образ в едином файле) подключение диска эмулируется специальной программой. Такие функции есть в «EnCase» и другом экспертном ПО.

Изучение архивов электронной почты и ICQ

На персональном компьютере сохраняется вся отправляемая и принимаемая корреспонденция. В зависимости от настроек, она может храниться долго или не очень или стираться сразу по прочтении. Но в любом случае, при получении и отправке информация записывается на диск хотя бы раз. А это значит, что если не в явном, то в скрытом виде она может найтись при экспертизе.

Средний пользователь хранит в архиве одну-две сотни сообщений электронной почты. Более активные пользователи могут хранить несколько тысяч. Вместе с копиями этих сообщений, вместе с удаленными сообщениями может получиться очень много информации. Не хватит никакой бумаги, чтобы всю ее распечатать. Поэтому никогда не следует давать задание эксперту найти и отпечатать всю найденную электронную переписку.

С другой стороны, сводить работу эксперта к обнаружению одного-двух заданных писем тоже неверно. Лучше всего поставить перед экспертом вопрос об обнаружении всей переписки как в явном, так и в скрытом (удаленном) виде.

Те сообщения, которые относятся к делу, следует распечатать на бумаге и приложить к заключению. Весь прочий архив переписки имеет смысл записать на компакт-диск. Если окажется, что распечатанного недостаточно, не надо будет проводить повторную экспертизу, достаточно

всего лишь провести осмотр содержимого компакт-диска, записанного экспертом. Для осмотра архива электронной почты или ICQ, записанного в каком-либо распространенном формате (например, текстовом), не требуется специальных знаний. Такой осмотр может провести следователь с понятыми. Кроме того, исследованный компьютер после хранения может оказаться и непригоден для повторного исследования – условия хранения вещественных доказательств у нас не самые оптимальные. А информация на компакт-диске, который приложен к заключению эксперта и хранится прямо в уголовном деле, – это надежнее и проще.

Решать, какая именно часть переписки относится к делу, целесообразно поручить эксперту. Для этого его необходимо ознакомить с материалами дела. В простейших случаях бывает достаточно изложить фабулу дела в постановлении о назначении экспертизы.

Кроме обнаружения архива переписки нужно поставить вопрос о том, принимались ли (отправлялись ли) найденные сообщения. Электронное письмо попадает в архив не только в том случае, когда оно отправлено с данного компьютера или принято на данный компьютер. Оно может быть записано (импортировано) в архив по особой команде пользователя. Оно может быть приложено к другому письму, которое поступило пользователю. Многие люди, когда меняют компьютер, переписывают со старого на новый весь архив электронной почты. Различные следы скажут эксперту, было ли найденное сообщение принято или отправлено при помощи исследуемого компьютера, или оно принималось/отправлялось из другого места, а на исследуемый диск попало каким-то иным путем.

Факт отправки или приема электронного сообщения нельзя строго доказать одним только обнаружением его на компьютере отправителя или получателя в ходе экспертизы. Необходимо подтвердить факт передачи письма «на другом конце» или на промежуточном узле. Иногда второй корреспондент известен. Но часто местоположение второй копии письма выясняется лишь в ходе проведения экспертизы. В таких случаях бывает полезно поставить перед экспертом вопрос, где еще можно обнаружить копию сообщения или следы его передачи.

Реконструкция просмотра веб-страниц

Из тех следов просмотра пользователем веб-сайтов (веб-сёрфинга), которые могут быть обнаружены на пользовательском компьютере, следует отметить cookie-файлы, историю просмотра и кэш браузера (временные файлы). Также при анализе следует учитывать хранимые браузером пароли к сайтам и закладки.

История просмотра веб-страниц – это, упрощенно говоря, перечень адресов (URL) веб-сайтов, к которым пользователь осуществлял доступ.

Одни браузеры хранят историю в своих настройках, другие – вместе с временными файлами.

Кэш браузера (временные файлы) – это копии HTML-файлов, изображений и иных файлов, загружаемых в ходе просмотра веб-страниц. Они сохраняются на локальном диске на случай повторного просмотра тех же страниц. Вместе с каждым файлом принимается и записывается срок его актуальности.

В cookie-файлах содержится адрес веб-сайта, который создал этот файл, значения переменных, время создания и срок актуальности этого cookie. Эти файлы сохраняются на компьютере пользователя по инициативе веб-сервера и предназначены, для того чтобы сервер мог сохранить индивидуальные настройки пользователя [71, 72].

Все описанные данные, если они сохранились, позволяют в подробностях восстановить последовательность просмотра пользователем веб-сайтов. Эта процедура может быть автоматизирована. Реконструкцию веб-сёрфинга по сохраненным данным браузера выполняют экспертные программы «EnCase», «FTK», «Pasco» и некоторые другие. Реконструкцию можно провести и вручную.

В свете изложенного вполне уместно выглядит такой вопрос эксперту: «Восстановить последовательность просмотра пользователем веб-сайтов в такой-то период времени» или «Установить, когда пользователь просматривал веб-сайт такой-то, в какой последовательности и какую информацию при этом получал».

Учитывая, что достаточно распространены веб-интерфейсы к электронной почте, при помощи восстановления просмотренных пользователем веб-страниц можно установить получение и отправку им сообщений электронной почты через такой веб-интерфейс.

Оценка найденного

Распространенной ошибкой следствия является поставить перед экспертом вопрос о наличии на НЖМД того или иного содержимого, но не поинтересоваться, каким образом найденная информация там оказалась. Добросовестный эксперт, конечно, сам, без дополнительного вопроса, укажет в заключении, каким путем найденная информация образовалась на диске.

Многие следователи и судьи молчаливо предполагают, что если информация найдена в компьютере, то именно пользователь компьютера поместил ее туда. Это не всегда так. Существует ряд путей, когда интересующая следствие информация попадает в компьютер помимо воли и без ведома его пользователя. Перечислим эти пути:

- НЖМД*, прежде чем попасть в исследуемый компьютер, мог использоваться в другом, у другого пользователя. Продаются подержанные жесткие диски. Даже если диск (компьютер) куплен в магазине и считается «новым», не исключено, что он был возвращен в торговую сеть предыдущим покупателем. Некоторые предприятия-сборщики компьютеров для экономии используют подержанные комплектующие, не уведомляя об этом потребителей. Подержанная электроника с виду ничем не отличается от новой. Конечно, продавец, как правило, переразмечает и/или переформатирует НЖМД. Но прежняя информация при этом на диске остается и будет обнаружена в ходе экспертизы.
- Вредоносные программы, от которых никто не застрахован[1], скрытно внедряясь на компьютеры, часто открывают «черный ход», позволяющий как снимать информацию по сети с этого компьютера, так и записывать на него. Указанным «черным ходом» может воспользоваться как «хозяин» вредоносной программы, так и иное лицо. Поскольку особенности устройства и поведения всех выявленных вредоносных программ известны, находится немало желающих воспользоваться ресурсами скомпрометированных компьютеров для собственных целей. Злоумышленники постоянно сканируют Интернет в поисках известных «черных ходов», а найдя, пытаются получить контроль над компьютером, присоединив его к своей зомби-сети*. Плотность сканирования достаточно высока. Компьютер с известной уязвимостью, будучи «выставлен» в Интернет без защиты, заражается вредоносной программой в течение считанных минут. Описанным способом на диске скомпрометированного компьютера может образоваться информация без желания и ведома его пользователя.
- При просмотре веб-сайтов вся полученная браузером информация в том или ином виде откладывается на жестком диске. Попасть на веб-сайт пользователь может и без своего желания, будучи автоматически перенаправлен или завлечен обманом. На сайте могут размещаться рекламные баннеры*, содержание которых владелец сайта не контролирует. Кроме того, на диск (в кэш браузера) записывается не только просмотренная пользователем информация, но и такая, которую он даже не видел – не пролистал веб-страницу до конца, не дождался ее окончательной загрузки, не активировал скрипт, быстро закрыл всплывающее (pop-up) окно и так далее. То есть пользователь не видел информации и не желал ее получать, а эксперт нашел такую информацию на диске.
- Примерно то же относится к спаму*. Полученный пользователем без его желания спам, хотя и стирается, зачастую даже без беглого прос-

[1] Доказано, что своевременное обновление всего ПО и постоянное использование антивирусной программы, хотя и снижает риск заражения, но отсутствия вирусов не гарантирует. Обновления (патчи) к ПО и новые базы к антивирусам выходят несколько позже, чем соответствующие вирусы.

мотра, сохраняется на диске. Его содержимое наверняка будет найдено при проведении экспертизы и при неверном истолковании может привести к судебной ошибке. Известно, что в спаме часто рекламируются незаконные товары и услуги.

- Персональный компьютер редко используется человеком строго персонально. Члены семьи, друзья и коллеги вполне могут время от времени воспользоваться чужим персональным компьютером, чтобы нечто скачать с Интернета или переписать информацию с одного носителя на другой. Часто это делается без ведома владельца. Поэтому всегда остается вероятность найти на диске информацию, к которой пользователь не имеет отношения.
- Компьютеры иногда отдают в ремонт. В ходе диагностики и ремонта на диск может устанавливаться специализированное ПО (в том числе двойного назначения) и записываться всякая информация в тестовых целях. Конечно, тестовую информацию удалят, но впоследствии, в ходе экспертизы, она будет обнаружена и может быть неверно интерпретирована.

Автор вовсе не хочет сказать, что все, обнаруженное на компьютере подозреваемого, следует списывать на вирусы, спам и прежних владельцев. Как правило, эксперт в состоянии определить, когда, каким способом и в каком контексте найденная информация была записана на диск – и тем самым развеять сомнения относительно ее происхождения. Перед экспертом наряду с вопросом о присутствии на диске той или иной информации всегда надо ставить вопрос о том, каким способом и при каких обстоятельствах эта информация там оказалась.

Исследование программ

Когда заходит речь об исследовании создания программ для ЭВМ, сравнении двух программ, установлении соответствия исходного кода и исполняемого кода – словом, когда исследование не может ограничиться «внешней» функциональностью программ, то требуются специальные знания в области программирования. Специалист в сфере информационных технологий, компьютерных сетей, защиты информации и специалист в области программирования редко сочетаются в одном лице. Как правило, программист имеет лишь общие представления об ИТ и наоборот.

Поэтому, если требуются глубокие знания по программированию, стоит назначить по этому вопросу отдельную экспертизу.

Например, лицо подозревается в создании (именно создании, не модификации) вредоносной программы и получении с ее помощью конфиденциальных данных с компьютера потерпевшего. Доказательства, очевидно, могут быть найдены на компьютере подозреваемого в ходе проведения КТЭ. Имеет смысл назначить две отдельные экспертизы либо одну

комплексную экспертизу. Первый эксперт (специалист по ИТ) должен разыскать на изъятом компьютере тексты программ и исполняемый код, а также ответить на вопросы о наличии конфиденциальной информации из компьютера потерпевшего. А второй эксперт (программист) должен исследовать найденный исходный код и исполняемый код вредоносной программы и ответить на вопросы, касающиеся ее устройства, функциональности, изготовления и авторства.

Изучение печатных документов

С какой-то точки зрения лист бумаги, вышедший из принтера, тоже является носителем компьютерной информации. Хотя такая информация предназначена для восприятия человеком, но записана она была при помощи компьютера. То, что напечатано на принтере, неизбежно было представлено в цифровом виде. Поэтому все распечатки следует рассматривать наравне с электронными носителями.

На распечатках содержится не только информация, ориентированная на человека. Машинная информация там тоже есть.

Изготовители принтеров из США закладывают в них печать на каждой странице скрытых данных о дате, времени и заводском номере принтера. Сделано это было по настоянию властей, но информация почти сразу стала широко известна [W14]. В том числе опубликованы места печати скрытой информации и ее кодировка [W15, W16, W17]. Информация эта, разумеется, неофициальная. Но ее несложно будет проверить в ходе экспертизы. Достаточно на том же принтере или на принтере такой же модели распечатать контрольную страницу (чистый документ) и сравнить обнаруженные на ней скрытые коды с кодами на исследуемом документе.

Сведений о распечатке подобной скрытой сигнатуры принтерами, произведенными в других странах, нет.

Кроме нарочно созданных сигнатур у принтеров имеются индивидуальные особенности и особенности, присущие модели [47]. Поэтому экспертиза может не только привязать печатный документ к конкретному принтеру, но и по документу установить, на принтере какой модели он был напечатан.

Стоимость ПО

Несколько слов про иной вид экспертизы, необходимый при расследовании компьютерных преступлений.

На квалификацию преступления по ст. 146 (ч.ч. 2 и 3) УК влияет стоимость экземпляров или прав на использование произведения. Автор хотел бы лишний раз подчеркнуть, что в статье фигурирует именно **стоимость**. Не ущерб и не цена. Довольно часто на следствии происходит путаница (а то и

умышленная подмена понятий): эксперту ставят вопрос об ущербе правообладателю, в качестве доказательства приводят справку о цене программного продукта. В то время как оценить следует именно его стоимость.

Как известно, стоимость товара или услуги является объективной категорией. То есть она не определяется желаниями участников конкретной сделки, не зависит от мнения автора или правообладателя. Упомянутые субъекты могут устанавливать только цену конкретной сделки. А стоимость зависит от состояния рынка в целом, от полезности товара и других объективных категорий.

Поскольку стоимость объективна, ее можно оценить. Оценку стоимости в идеале должен проводить эксперт-экономист или эксперт-оценщик [L04]. Разумеется, эксперт должен быть независим от автора или правообладателя. **Оценку стоимости не может проводить потерпевший.** Хотя, к большому сожалению, в российской практике часто именно так и поступают – принимают в качестве стоимости прав на ПО сумму, декларированную потерпевшим.

Оценка стоимости программного обеспечения (точнее, прав на его использование) имеет свои особенности. Производство ПО с экономической точки зрения довольно сильно отличается от производства материальных товаров. Общие издержки на производство серии товара составляют почти 100%, а индивидуальные издержки на производство каждого экземпляра составляют ничтожную часть всех издержек. Отсюда и особенности в определении стоимости одного экземпляра ПО.

Другие экономические особенности программных продуктов таковы:

- Цена на ПО очень вариабельна. В зависимости от региона, потребителя, условий эксплуатации цена на одну и ту же программу может запросто отличаться в 10 и более раз. Нередки случаи, когда при определенных условиях или для определенных категорий пользователей лицензия на ПО вообще передается бесплатно, в то время как для прочих она стоит существенных денег.
- При выходе новой версии программы прежняя версия либо вовсе снимается с продажи, либо очень сильно дешевеет. В то время как цена новой версии обычно близка к прежней цене старой. Потребительские свойства более старой версии при этом не меняются.
- Часто новая версия программы (обновление до более новой версии) входит в цену старой, то есть легальным пользователям прежней версии ПО права на новую версию предоставляются бесплатно или с очень большой скидкой.
- Цена, как правило, нелинейно зависит от числа копий (инсталляций, пользователей). Например, лицензия на 1 копию стоит 1 условную единицу, на 20 копий стоит 10, на 50 копий – 20. В случае, когда использована 21 копия, их стоимость можно оценить в 10,5 условных единиц, в 11, в 20 или даже в 21.

- Некоторые программы могут вообще не продаваться в какой-то стране, хотя и пользоваться там некоторым спросом.
- Правообладатели порой бесплатно распространяют версию ПО с урезанными функциями или ограниченным сроком действия (так называемые пробные, ознакомительные, тестовые или триальные версии), но при этом такая ограниченная версия вполне удовлетворяет все потребности пользователя. Бывает, что пробная версия и полноценная версия программы устанавливаются с одного и того же дистрибутива и начинают отличаться друг от друга только с момента регистрации.
- Программы могут не продаваться без соответствующего оборудования или вне определенного комплекта программ. Но при этом сохраняется техническая возможность использовать их отдельно. В таком случае официальная цена на отдельную программу либо вообще не объявляется, либо выставляется в 0. Стоимость при этом далеко не нулевая.

Исходя из упомянутых сложностей, автор рекомендует для оценки стоимости прав на использование программы для ЭВМ назначать не экономическую, а комплексную экспертизу, с участием двух экспертов – экономиста и ИТ-специалиста. Особенно, когда оценка осложнена такими обстоятельствами, как использование устаревшей, изъятой из продажи версии ПО, использование версии, лицензируемой бесплатно для некоторых категорий, превышение количества инсталляций и т.д.

Конечно, не по каждому делу о нарушении авторских прав обязательно проводить экспертную оценку стоимости ПО. Иногда стоимость можно оценить без эксперта, исходя из цены. Если определенная программа продается (лицензируется) по одинаковой цене для всех или подавляющего большинства потребителей, то такую цену можно считать ее стоимостью. При наличии нескольких цен для различных условий следователь или суд может принять в качестве оценки наименьшую из этих цен.

Распространенные ошибки при оценке стоимости контрафактных программ или иных произведений, из опыта автора, таковы:

- из нескольких действующих цен на продукт в качестве оценки стоимости берется одна, причем выбор никак не обосновывается;
- в качестве оценки стоимости продукта берется цена на другую версию продукта – более новую, более старую, на другом языке и т.д.;
- оценка стоимости произведения (прав на его использование) поручается компьютерно-технической экспертизе;
- вместо стоимости оценивается цена продукта или ущерб правообладателю;
- оценка стоимости поручается правообладателю или производится следователем из данных, предоставленных правообладателем (например, фирменного каталога цен);
- при оценке стоимости через цену не учитываются условия, в которых

обвиняемый использовал программу, например, не учитывается наличие в лицензионном договоре скидок, льгот, периода бесплатного использования.

Но главной и самой распространенной ошибкой, разумеется, является оценка стоимости без проведения экспертизы.

Разбор образцов

В этой главе мы рассмотрим образцы заключений эксперта, подробно разберем их и укажем на ошибки.

Автор предлагает три экспертных заключения. Все они взяты из реальных уголовных дел, рассмотренных в суде. Первый пример изобилует ошибками, второй имеет всего несколько недостатков, а третий пример почти идеален и может быть рекомендован в качестве образца.

Отрицательный пример

Первое заключение взято из уголовного дела по статьям 146 и 273 УК. Исследование проводил эксперт Центра независимой комплексной экспертизы и сертификации (ЦНКЭС). Полный текст заключения приводится на последующих иллюстрациях.

Для начала рассмотрим поставленные перед экспертом вопросы.

Первый вопрос поставлен правильно. Речь можно вести не о контрафактности, а именно о признаках контрафактности. Сам факт контрафактности (то есть нарушения авторских прав) эксперт установить не может. Так что вопрос сформулирован верно, разве что формулировка немного корявая. Контрафактными (согласно определению из ст. 48 закона «Об авторском праве...») бывают не диски или иные носители, а записанные на них экземпляры произведений. Ну и термин «CD-диск», хотя и понятен, но звучит не вполне по-русски: говорят либо «CD», либо «компакт-диск».

Второй и пятый вопросы (они фактически идентичны) автор переформулировал бы иначе. Дело в том, что правообладатель – это владелец имущественных авторских прав, каковые права являются отчуждаемыми. То есть правообладатель может измениться, если будет заключен соответствующий договор, но произведение при этом не изменится ни на бит. Иными словами, «лицо является правообладателем» – это факт не технический, а юридический. Эксперт, как и в предыдущем случае, может лишь обнаружить признаки или какие-либо указания, что лицо является обладателем исключительных прав на произведение, но не может установить факт обладания такими правами.

Третий и шестой вопросы откровенно юридически безграмотны и неприемлемы для КТЭ. Во-первых, эксперт не может установить контрафактность произведений. Во-вторых, при нарушении авторских прав

нельзя вести речь об ущербе. При незаконном воспроизведении или ином использовании произведений у правообладателя ничего не пропадает, поэтому ущерба как такового нет. Можно вести речь о недополученной прибыли или иных убытках, но оценить их достаточно сложно. Именно поэтому законодатель оперирует в ст. 146 УК понятием «стоимость». Именно стоимость экземпляров или прав на их использование является квалифицирующим признаком этого преступления. Если экс-

НА РАЗРЕШЕНИЕ ЭКСПЕРТА ПОСТАВЛЕНЫ СЛЕДУЮЩИЕ ВОПРОСЫ:

1. **Имеют ли представленные на исследование экземпляры CD-дисков признаки контрафактности, если да, то какие?**
2. **Кто является правообладателем данной продукции?**
3. **Если представленные на исследование экземпляры нелицензионные (контрафактные), то какой ущерб причинен правообладателям?**
4. **Является ли программное обеспечение, установленное на представленных жестких дисках, лицензионным?**
5. **Кто является правообладателем продукции программного обеспечения, установленного на данных жестких дисках?**
6. **Если программное обеспечение, установленное на представленных жестких дисках нелицензионное (контрафактное), то какой ущерб причинен правообладателям?**
7. **Находятся ли на представленных на исследование экземплярах CD-дисках и жестком диске (HDD) вредоносные программы? Если находятся, то могли ли они быть применены для модификации программных продуктов, установленных на жестком диске и произошла ли указанная модификация?**

НА ЭКСПЕРТИЗУ ПРЕДСТАВЛЕНЫ:

- Внутренний жесткий диск Seagate Barracuda, опечатанный полоской белой бумаги с подписями.
- Переносной жесткий диск CUTIE FHD-254, опечатанный полоской белой бумаги с подписями.
- Два CD диска, упакованные в пластиковый бокс, опечатанные полосками белой бумаги с подписями.

ЭКСПЕРТИЗА:

Экспертиза проводилась в помещении ЦНКЭС.

Перед началом экспертизы было произведено вскрытие печатей на упаковке с носителями для возможности съема информации на магнитные носители.

Экспертиза проводилась в два этапа: первый - экспертиза компакт-дисков и переносного жесткого диска, второй – экспертиза внутреннего жесткого диска.

Этап № 1. Экспертиза CD – дисков и переносного жесткого диска:

перт возьмется оценивать ущерб, он вынужден будет признать, что ущерб нулевой, а стоимость при этом не будет оценена, что затруднит или сделает невозможной квалификацию деяния.

Четвертый вопрос также относится к контрафактности экземпляров. Термин «лицензионный» употребляется в обиходе как антоним к термину «контрафактный». А контрафактность экземпляров, как уже неоднократно подчеркивалось, эксперт установить не может. Поэтому данный вопрос сформулирован некорректно.

Седьмой вопрос в первой своей части поставлен правильно и относится к области КТЭ. Во второй своей части вопрос содержит скрытое утверждение, что вредоносные программы используются для модификации программных продуктов, то есть программ для ЭВМ. На самом деле вредоносные программы используются для модификации не произведений, а компьютерной информации, и указанные отношения регулируются законодательством об информации [70, 81]. А использование программ для ЭВМ регулируется законодательством об авторском праве, в сферу которого вредоносные программы (ст. 273 УК) не входят. Речь можно вести лишь о программном обеспечении для преодоления технических средств защиты авторских прав (ст. 48.1 закона «Об авторском праве...»). Поэтому вторая часть вопроса 7 некорректна.

Перейдем к разбору самого заключения.

Ввиду отсутствия необходимого оборудования, необходимого для подключения переносного жесткого диска к системному блоку Центра, экспертиза переносного жесткого диска CUTIE FHD-254 не проводилась.

На исследование представлены следующие компакт – диски:

Таблица 1.

№ п/п	Наименование (внешний вид) компакт - диска
1.	Весь Autocad 2006
2.	№ A4408G5061902

В результате проведения экспертизы установлено, что представленные компакт – диски №№ 1,2 таблицы № 1 имеют существенные отличия от лицензионных (изготовленных и реализуемых с соблюдением всех требований законодательства РФ в части авторского права) компакт-дисков. Соответствующий вывод сделан по результатам осмотра внешнего вида, а также файловой структуры данных компакт-дисков при помощи загрузки в память ЭВМ записанных на них программ. Данные компакт-диски и программные продукты, содержащиеся на них, имеют явные признаки контрафактности.

Список компьютерных программ, имеющих явные признаки контрафактности и расчет их стоимости, приведены в **Таблице 2.**

АНО «ЦНКЭС» ЭКСПЕРТИЗА
подпись эксперта

Таблица 2.

№ п/п	Наименование (внешний вид) компакт - диска	Наименование программного продукта	Право обладатель	Стоимость,
1.	Весь Autocad 2006	AutoCAD 2004	AutoDesk	Нет данных
		AutoCAD 2005	AutoDesk	2 160 Евро
		AutoCAD 2006	AutoDesk	4 320 Евро
2.	№ A4408G5061902	Windows XP Professional Russian	Microsoft	251 у.е.*

*1 у.е = 1 доллару США по курсу ЦБ РФ на день изъятия дисков.
Цены взяты из «Справочника цен на лицензионное программное обеспечение», разработанного Некоммерческим Партнерством Поставщиков Программных Продуктов (НП ППП).

Признаки контрафактности компакт – дисков, представленных на исследование, следующие:

1. Оформление лицевой (нерабочей) поверхности лицензионных компакт-дисков.

На лицевую (нерабочую) поверхность лицензионного компакт-диска наносится изображение высокого полиграфического качества. По окружности внешней границы компакт-диска должны быть нанесены: надпись, содержащая информацию о регистрации торговых марок, об авторском и смежных правах на данную программу для ЭВМ (базу данных) и предупреждение о последствиях их нарушения. Экспертиза показала, что представленные компакт-диски не имеют каких – либо изображений и текстовой информации о торговых марках, авторском и смежном праве.

2. Оформление реверса (рабочей поверхности) лицензионных компакт-дисков.

Оформление реверса (рабочей поверхности) компакт-диска. Вдоль концентрических окружностей в центре лицензионного компакт-диска наносится методом гравировки код **IFPI** (код Международной федерации производителей фонограмм), позволяющий однозначно идентифицировать оборудование, на котором изготовлен данный компакт-диск, а также информация о заводе-изготовителе.

У представленных на экспертизу компакт-дисков код IFPI отсутствует. Производитель на компакт-дисках не указан.

Данные признаки являются существенными признаками контрафактности.

3. Упаковка лицензионных компакт-дисков.

АНО «ЦНКЭС» ЭКСПЕРТИЗА
подпись эксперта

4

Лицензионные программы для ЭВМ, как правило, упаковываются в картонную коробку, оформляемую согласно стандартам фирмы-изготовителя, имеющую несколько степеней защиты (микро печать, голограммы и т.п.). На коробке должна присутствовать информация о фирме-разработчике, авторских и смежных правах. Кроме того, в упаковочную коробку вкладывается многостраничная документация (инструкция пользователя) и лицензия на программный продукт.

Лицензионные программы для ЭВМ компании Microsoft упаковываются в картонные коробки, типоразмеры и оформление которых соответствуют корпоративным стандартам производителя и имеют несколько степеней защиты. Неотъемлемой частью каждого продукта является Лицензионное соглашение между покупателем и фирмой-производителем. Каждая Лицензия или Регистрационная карта пользователя имеет серийный номер программного продукта, без которого установка программного продукта невозможна. Представленные на экспертизу компакт-диски с программами данной фирмы таких компонентов не содержит.

На боковой стороне картонной коробки с программами Майкрософт имеется специальный сертификат, имеющий следующие свойства:

- теплочувствительная краска при трении изменяет цвет с голубого на белый;
- попытка отклеить сертификат вызывает его разрыв;
- поворот сертификата в лучах света обнаруживает символ "ОК" на логотипе Майкрософт.

Представленные на экспертизу компакт-диски с программными продуктами фирмы Майкрософт в момент осмотра не были упакованы, не имели картонных упаковочных компонентов, документации, лицензий и регистрационных карточек.

Описание комплекта AutoCAD:

Коробка

- Размеры коробки продукта—примерно 17.8 x 22.8 см. Толщина коробки может составлять 5, 7, 7.6, 12.7 или 15.2 см.
- Версии с Release 14 по 2000 поставлялись в картонных коробках, одна половина которых вставлялась в другую сбоку. Начиная с семейства 2002, коробка открывается сверху и имеет сплетение клапанов на дне.
- Серийный номер и сведения о продукте находятся, как правило, на верхнем клапане.
- Шифр продукта и текст с правовой информацией находятся на дне коробки.

5

При анализе внешних признаков контрафактности компакт-дисков (с. 3-6) они были сопоставлены и сравнены с некими «лицензионными» дисками. Но образцы таких дисков для сравнения эксперту следователем не предоставлялись. А согласно ст. 57 УПК, эксперт не вправе самостоятельно собирать материалы для экспертного исследования; такие образцы должны быть направлены эксперту следователем в числе прочих материалов, необходимых для производства экспертизы, либо по отдельному запросу эксперта.

Кроме того, программные продукты выпускаются на рынок в различных вариантах и различном исполнении. Наряду с «коробочными» версиями (они же «retail» или «розничные») возможны OEM-версии, версии, распространяемые через Интернет, и иные варианты, всего многообразия которых эксперт может не знать. Даже сам правообладатель может не знать, в каком оформлении выпускают его программный продукт издатели, с которыми он заключил договоры. Поэтому непохожесть исследуемых дисков на диски «коробочной» версии продукта еще не есть признак контрафактности.

Чтобы внешний вид экземпляра стал признаком контрафактности, следует сравнить его с внешним видом всех имевших место официальных изданий всех издателей во всех странах. Сравнение лишь с одним-единственным образцом – некорректно.

Указание экспертом правообладателя является логическим продолжением ошибки следователя в постановке вопроса. Эксперт не может определить правообладателя произведения, поскольку это факт юридический, а не технический. Принадлежность имущественных авторских прав тому или иному лицу зависит от заключенных договоров и от факта создания произведения тем или иным лицом (лицами). Эксперт же исследует лишь экземпляр произведения. Поэтому он может найти на произведении сведения об авторах, уведомление о принадлежности авторских прав, текст лицензионного соглашения и иные признаки. Но лишь признаки. Из которых однозначный вывод о правообладателе сделать нельзя.

- Серийный номер продукта и текст с правовой информацией находятся на дне коробки

Содержимое коробки

Содержимое коробки зависит от конкретного продукта; ниже перечислены требования, общие для всех них:

- Большинство печатных руководств имеет формат 17.8 x 22.8 см и стандартный мягкий переплет. Обратите внимание, что для тонких книг такой переплет невозможен, и они обычно бывают скреплены по сгибу.
- На задней стороне обложки печатных руководств обязательно должен быть заводской шифр.
- Все содержимое коробки (начиная с семейства 2002) подчиняется единой цветовой схеме.

Компакт-диск

- CD упакован в картонный или гибкий пластиковый конверт; все надписи на конверте нанесены методом офсетной печати.

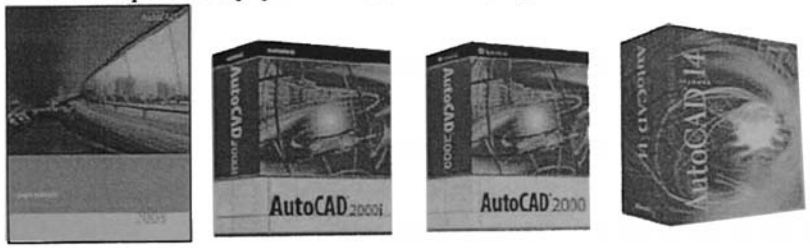
Примечание: AutoCAD 14 был последним продуктом, диск которого поставлялся в твердом пластмассовом футляре.

- Этикетка нанесена на диск методом шелкографии.

Примечание: Если этикетка отклеивается с диска, это свидетельствует о подделке.

- На внутреннем кольце CD нанесены номер партии и наименование завода-изготовителя тиража.

Ниже проиллюстрированы подлинные продукты компании Autodesk.



Представленный на экспертизу компакт-диск с программным продуктом фирмы Autodesk в момент осмотра был упакован в пластиковый бокс, не имел картонных упаковочных компонентов и документации.

Все эти признаки являются признаками контрафактности.

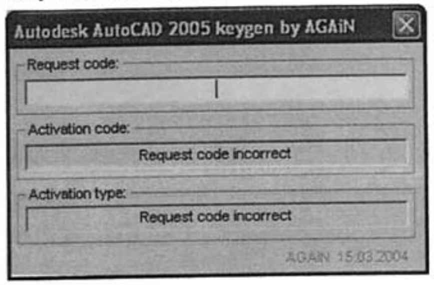
4. Наличие программ устраняющих защиту от несанкционированного копирования.

6

На компакт-диске не могут быть записаны программы для ЭВМ, позволяющие устранить либо обойти защиту от несанкционированного копирования.

На компакт-дисках находятся файлы вредоносных программ, позволяющие обойти встроенную в программные продукты средства защиты от несанкционированного копирования и получить тем самым незаконный доступ к программным продуктам компании AutoDesk и компании Adobe, что является существенным признаком контрафактности представленных компакт-дисков с программными продуктами данных компаний.

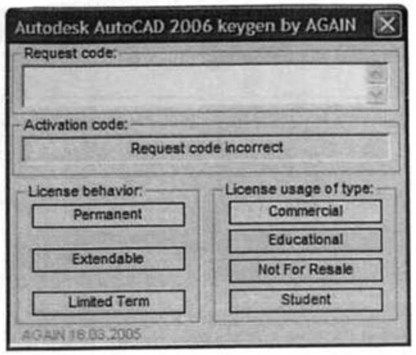
На компакт – диске «Весь Autocad 2006» в директории «..\Autocad 2005 RUS» обнаружен самораспаковывающийся файл-архив «AutoCAD2005Rus.exe», содержащий файл программы «keygen.exe». При запуске данного файла появляется следующий оконный интерфейс:



Установлено, что данная программа предназначена для генерации кода активации (не активированная копия программного продукта работать не будет) программного продукта «AutoCAD 2005» без ведома правообладателя – компании «AutoDesk» (т.е. с помощью программы можно осуществить доступ к компьютерной информации и копирование информации). На основании данного факта программа ««keygen.exe»» признана **вредоносной**.

На компакт-диске Весь Autocad 2006» в директории «..\AutoCAD 2006 Rus\Crack» обнаружен файл программы «keygen.exe». При запуске данного файла появляется следующий оконный интерфейс:

7



Установлено, что данная программа предназначена для генерации кода активации (не активированная копия программного продукта работать не будет) программного продукта «AutoCAD 2006» без ведома правообладателя – компании «AutoDesk» (т.е. с помощью программы можно осуществить доступ к компьютерной информации и копирование информации). На основании данного факта программа «keygen.exe» признана **вредоносной**.

Этап № 2. Экспертиза жесткого диска.

Экспертиза представленного жесткого диска проводилась по следующей методике:

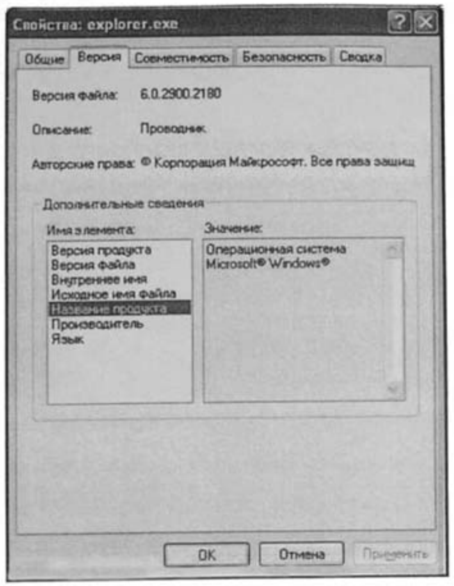
Жесткий диск был подключен к системному блоку Центра, после чего производился поиск информации, необходимой для ответа на поставленные вопросы.

В результате проведения экспертизы жесткого диска установлено:

На жестком диске в директории «C:\WINDOWS» обнаружен программный продукт Microsoft Windows XP Professional Russian, правообладатель компания Microsoft.

К признакам контрафактности обнаруженной операционной системы можно отнести факт возможной установки данной операционной системы с представленного на экспертизу компакт – диска № «A4408G5061902» (содержащего дистрибутив (установочные файлы) данной операционной системы, имеющего явные признаки контрафактности).

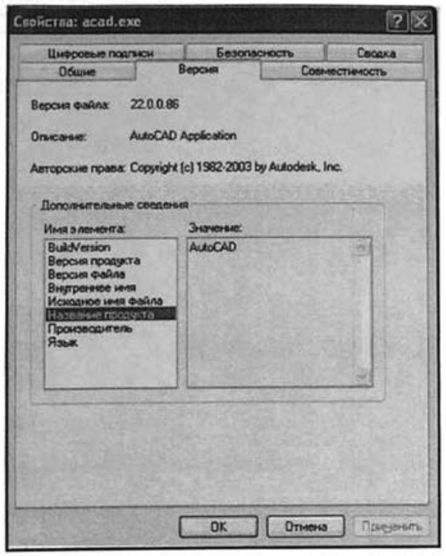
АНО «ЦНКЭС» ЭКСПЕРТИЗА
подпись эксперта



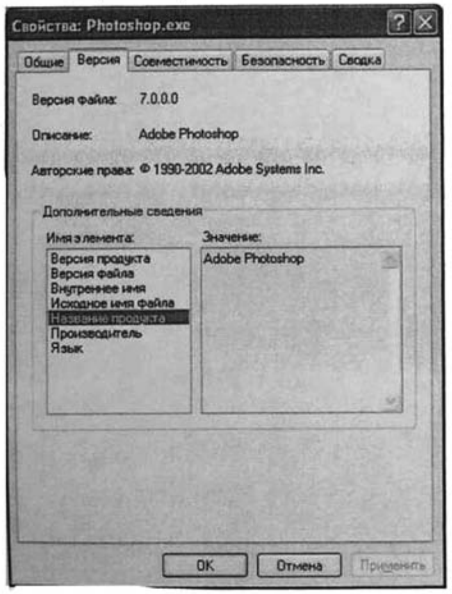
На представленном жестком диске в папке «C:\Program Files\AutoCAD 2005» обнаружен программный продукт «AutoCAD 2004» правообладатель компания «Autodesk». К признакам контрафактности данного программного продукта можно отнести возможный факт его установки с компакт – диска «Весь Autocad 2006», представленного на экспертизу, имеющего явные признаки контрафактности.

АНО «ЦНКЭС» ЭКСПЕРТИЗА
подпись эксперта

Ряд иллюстраций, приведенных экспертом, не подписаны и не объяснены в тексте. У неспециалиста может создаться впечатление, что эти иллюстрации подтверждают правоту эксперта. На самом деле это не так.



На представленном жестком диске в папке «..\Program Files\Adobe\Photoshop 7.0» обнаружен программный продукт «Adobe Photoshop 7.0» правообладатель компания «Adobe».

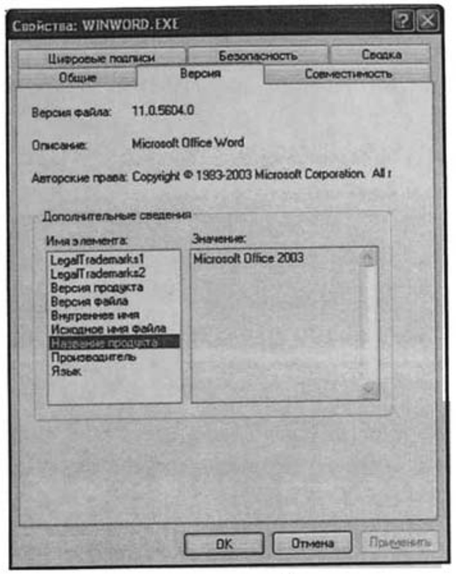


10

Например, иллюстрация на странице 10 – это результат отображения некоторых атрибутов файла средствами операционной системы. Строчка «авторские права...» является лишь частью контента (ресурсов) файла «Photoshop.exe». Ее можно рассматривать как признак принадлежности авторских прав или как уведомление о таких правах. Но эксперт этого не объясняет. Он категорично утверждает «правообладатель – компания «Adobe», после чего приводит иллюстрацию, которую неспециалист может воспринять как подтверждение. Иными словами, отсутствие подписей к иллюстрациям вводит в заблуждение.

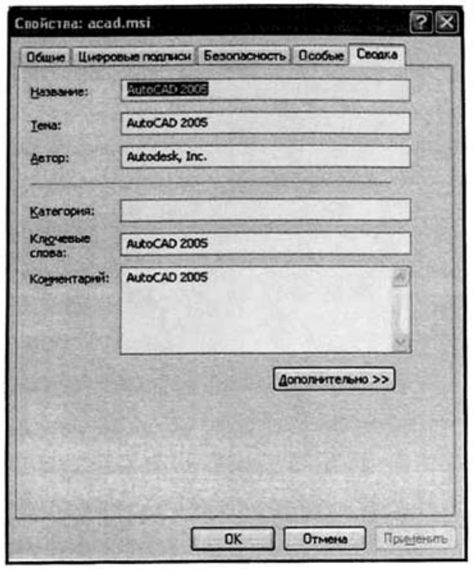
К признакам контрафактности данного программного продукта можно отнести возможный факт его установки с дистрибутива, имеющего признаки контрафактности, обнаруженного на представленном жестком диске (см. ниже).

В папке « ..\Program Files\Microsoft Office» обнаружен программный продукт «Microsoft Office 2003 Professional (Russian)», правообладатель компания Microsoft.

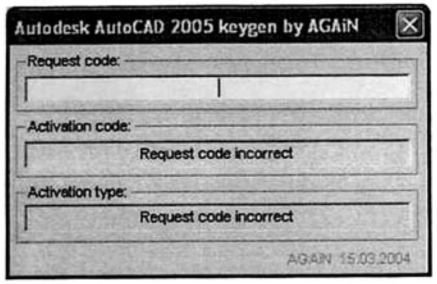


Признаков контрафактности данного программного продукта не обнаружено.

Так же на представленном внутреннем жестком диске в директории «..\Utils\Distrib\Autocad\Autocad 2005 RUS&ENG» обнаружен дистрибутив (установочные файлы) программного продукта «AutoCAD 2005» правообладатель компания «Autodesk».



Явным признаком контрафактности данного программного продукта является наличие в директории, содержащий программный продукт поддиректории «crack» в которой содержится файл «keygen.exe». При запуске данного файла появляется следующий оконный интерфейс:



Установлено, что данная программа предназначена для генерации кода активации (не активированная копия программного продукта работать не будет) программного продукта «AutoCAD 2005» без ведома правообладателя – компании «AutoDesk» (т.е. с помощью программы можно осуществить доступ к компьютерной информации и копирование информации). На основании данного факта программа ««keygen.exe»» признана **вредоносной**.

Так же к признакам контрафактности обнаруженного дистрибутива программного продукта «AutoCAD 2005» можно отнести возможный факт его копирования с компакт – диска «Весь Autocad 2006», представленного на исследование, имеющего явные признаки контрафактности.

12

На жестком диске в директории «..\Utils\Distrib\Photoshop 7» обнаружен дистрибутив (установочные файлы) программного продукта «Adobe Photoshop 7.0» правообладатель компания «Adobe».

К признакам контрафактности данного программного продукта можно отнести возможный тот факт, что данный программный продукт (в виде дистрибутива) распространяется официально только на компакт – дисках. На других носителях дистрибутив программного продукта «Adobe Photoshop 7.0» официально не распространяется.

Сравнительный анализ программного обеспечения, установленного на представленном жестком диске и дистрибутивов программных продуктов, записанных на представленных на исследование компакт-дисках и жестком диске, содержащих программные продукты, имеющие признаки контрафактности, показал, что обнаруженные на жестком диске программные продукты могли быть установлены (либо скопированы) с представленных на исследование компакт-дисков и переносного жесткого диска (в соответствии с обнаруженными на данных носителях дистрибутивами программных продуктов).

Информация о стоимости обнаруженных на представленном жестком диске программных продуктов, имеющих признаки контрафактности, приведена в Таблице 3.

Таблица 3.

Расчет стоимости программ, имеющих признаки контрафактности, обнаруженных на жестком диске, представленном на экспертизу

Программы, находящиеся на жестком диске	Правообладатель	Стоимость программного продукта
AutoCAD 2004	Autodesk	Нет данных
AutoCAD 2005 (дистрибутив)	Autodesk	2 160 Евро
Microsoft Windows XP Professional Russian	Microsoft	251 у.е.*
Adobe Photoshop 7.0	Adobe	Нет данных
Adobe Photoshop 7.0 (дистрибутив)	Adobe	Нет данных

*1 у.е = 1 доллару США по курсу ЦБ РФ на день изъятия жесткого диска.

Расчет стоимости программ

Для расчета стоимости программ принята следующая модель: для обнаруженного экземпляра программы с признаками контрафактности

13

Определение стоимости программ (прав на их использование) в соответствии с ценой является ошибкой. Тем более что из различных цен взята розничная, то есть максимальная.

Есть подозрение, что эксперт вообще не видит разницы между ценой и стоимостью. В тексте эти термины употребляются как синонимы.

определяется стоимость в соответствии с розничной ценой соответствующего лицензионного программного продукта на момент востребования носителей информации (компакт – дисков и жесткого диска).

В случае указания розничной цены программы в иностранной валюте, пересчет в рублевый эквивалент осуществляется по курсу ЦБ РФ на день изъятия информационных носителей.

Стоимость программ рассчитывалась по формуле **X * У = Z**, где

X- Общее количество контрафактных экземпляров программ,

У – Розничная цена экземпляра программы,

Z – Общая стоимость программ правообладателя.

Таким образом, стоимость программ на представленных компакт – дисках, составляет:

- компании «AutoDesk»:

6 480 (две тысячи сто шестьдесят) евро, что в пересчете согласно курсу ЦБ РФ на 07 июля 2006 г. (1 евро = 34 руб. 28,21 коп.) составляет 222 148 (двести двадцать две тысячи сто сорок восемь) рублей 01 коп.

- компании «Microsoft»:

251 (двести пятьдесят один) доллар 00 центов США, что в пересчете согласно курсу ЦБ РФ на 07 июля 2006 г. (1 доллар США = 26 руб. 91,11 коп.) составляет 6 754 (шесть тысяч семьсот пятьдесят четыре) рубля 69коп.

Стоимость программ, установленных на представленном внутреннем жестком диске, составляет:

- компании «AutoDesk»:

2 160 (две тысячи сто шестьдесят) евро, что в пересчете согласно курсу ЦБ РФ на 07 июля 2006 г. (1 евро = 34 руб. 28,21 коп.) составляет 74 049 (семьдесят четыре тысячи сорок девять) рублей 34 коп.

- компании «Microsoft»:

251 (двести пятьдесят один) доллар 00 центов США, что в пересчете согласно курсу ЦБ РФ на 07 июля 2006 г. (1 доллар США = 26 руб. 91,11 коп.) составляет 6 754 (шесть тысяч семьсот пятьдесят четыре) рубля 69коп.

подпись эксперта

ВЫВОДЫ:

1. В результате проведенной экспертизы на представленных компакт – дисках (позиции №№ 1,2 таблицы № 1) обнаружены программные продукты, имеющие признаки контрафактности. Программы на компакт-дисках имеют следующие признаки контрафактности:

- **отсутствие информация о торговых марках, а так же об авторском и смежных правах на лицевой поверхности;**
- **отсутствие полиграфического изображения на лицевой поверхности;**
- **отсутствие кода IFPI (код Международной федерации производителей фонограмм);**
- **отсутствие упаковочной коробки и документации;**
- **наличие на компакт-дисках вредоносных программ, позволяющих обойти защиту от несанкционированного копирования.**

2. Правообладателями обнаруженных программных продуктов на компакт-дисках являются корпорация «Microsoft», компания «AutoDesk».

3. Стоимость программ, на представленных компакт – дисках, составляет:

- компании «AutoDesk»:

222 148 (двести двадцать две тысячи сто сорок восемь) рублей 01 коп.

- компании «Microsoft»:

6 754 (шесть тысяч семьсот пятьдесят четыре) рубля 69коп.

4. Ввиду отсутствия необходимого оборудования, необходимого для подключения переносного жесткого диска к системному блоку Центра, экспертиза переносного жесткого диска CUTIE FHD-254 не проводилась.

Программные продукты, установленные на представленном на экспертизу жестком диске, имеют следующие признаки контрафактности:

- **Установка программных продуктов с компакт – дисков, представленных на экспертизу, содержащих программные продукты, имеющие явные признаки контрафактности.**
- **Наличие вредоносной программы в директории, содержащий программный продукт.**
- **Несоответствие типа носителя, содержащего дистрибутив (установочные файлы) программного продукта, носителю,**

подпись эксперта 15

Разберем выводы эксперта.

Целый раздел заключения эксперта посвящен анализу программ для обхода технических средств защиты авторских прав. Эксперт ошибочно объявляет их вредоносными программами. Это утверждение не основано на законе, поскольку такие программы не приводят заведомо к несанкционированному копированию, модификации или уничтожению информации [21, 81]. А такая программа, как генератор ключей активации, вообще не приводит к копированию, модификации или уничтожению какой-либо информации.

При поиске признаков контрафактности копии ОС «Windows», которая инсталлирована на исследуемом НЖМД, эксперт приводит единственный такой признак, дословно: «факт возможной установки данной операционной системы с представленного на экспертизу компакт-диска» (с. 8). Такой же, единственный признак контрафактности эксперт указывает для продукта «Photoshop» (с. 11). Других признаков контрафактности экземпляров этих программ эксперт не указывает. Однако в выводах (с. 15) при указании признаков контрафактности написано «установка программных продуктов с компакт-дисков», а слово «возможная» пропало. Итак, вывод относительно контрафактности «Windows» и «Photoshop» сформулирован экспертом категорично, хотя он основан на единственном признаке, который носит предположительный характер.

Оценка стоимости. Здесь эксперт исправил ошибку следователя, который ошибочно поставил вопрос об ущербе. Эксперт же отвечает на вопрос не об ущербе, а о стоимости прав на использование произведений.

Но оценка стоимости прав на использование соответствующих программ для ЭВМ может производиться в ходе экономической или товароведческой экспертизы. КТЭ не может дать такую оценку.

Кроме того, эксперт допустил ошибку, взяв цену на продукт «AutoCad» из справочника цен. Этот продукт имеет множество версий и несколько вариантов лицензий для разных условий его использования. Соответственно, нет и не может быть единой цены на этот продукт. Для данного уголовного дела ошибка эксперта усугубляется еще и тем, что лицензия на «AutoCad» предусматривает период бесплатного его использования, так называемое «trial use», или пробное использование. В этом режиме продукт инсталлируется с того же самого дистрибутива. Следовательно, стоимость прав на такой вид использования составляет ноль. Понятно, что не имеет смысла говорить о стоимости экземпляров или прав на использование программы для ЭВМ, пока не выяснено, каким именно способом программу использовали или намеревались использовать. Нет смысла говорить о стоимости без изучения условий лицензионного договора. Особенно когда договор предусматривает бесплатные варианты использования. Очевидно, что такие вопросы, как анализ лицензионного договора, технический эксперт решать не имеет права.

Автор сомневается, может ли данное заключение служить отрицательным примером для разбора возможных ошибок эксперта. Скорее, стоит вести речь не об ошибках, а о тенденциозности и ангажированности эксперта.

Тем не менее на основе этого примера сформулируем перечень типичных ошибок при назначении и проведении КТЭ:

- недопустимые вопросы перед экспертом (см. главу «Неприемлемые вопросы»);
- содержащееся в формулировке вопроса неявное утверждение;
- проведение техническим экспертом оценочной деятельности (экономической экспертизы);
- проведение техническим экспертом экспертизы по установлению автора (автороведческой экспертизы) или правообладателя;
- использование экспертом сравнительных образцов, полученных из неуказанного источника, вопреки установленному УПК порядку;
- путаница вредоносных программ и программ для обхода технических средств защиты авторских прав [21, 70, 81].

Промежуточный пример

Приведенное ниже заключение автор мог бы охарактеризовать как добросовестное, но проведенное без должной тщательности и без использования специальных технических средств.

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РФ
УПРАВЛЕНИЕ ВНУТРЕННИХ ДЕЛ КУРГАНСКОЙ ОБЛАСТИ
ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКОЕ УПРАВЛЕНИЕ

г. Курган, ул. С.Васильева, 30а тел. 41-60-75

ПОДПИСКА

Мне, Иванову Ивану Ивановичу, разъяснены в соответствии со ст. 199 УПК РФ права и обязанности эксперта, предусмотренные ст. 57 УПК РФ. Об ответственности за дачу заведомо ложного заключения по ст. 307 УК РФ предупрежден.

27 декабря 2002 г. И.И.Иванов

ЗАКЛЮЧЕНИЕ ЭКСПЕРТА №12

г. Курган 9 января 2003 года

Производство экспертизы
Начато в 10 ч.00 мин. 27 декабря 2002 г.
Окончено в 15 ч.40 мин. 9 января 2003 г.

Старший эксперт МЭКО при ЭКУ УВД Курганской области старший лейтенант милиции Иванов И.И., имеющий высшее образование и стаж экспертной работы четыре года, на основании постановления о назначении экспертизы, вынесенного 26 декабря 2002 года старшим следователем СЧ СУ при УВД Курганской области старшим лейтенантом юстиции Пуховой А.М., по материалам уголовного дела №123456 произвел судебную компьютерно-техническую экспертизу.

ОБСТОЯТЕЛЬСТВА ДЕЛА

18.12.02 г. у Остановочного комплекса «Спорткомплекс «Зауралец» у Лоськова обнаружена и изъята денежная купюра достоинством 50 рублей серии «яч 8080000» образца 1997 г. с признаками подделки. Предварительным следствием установлено, что данная купюра изготовлена на компьютерном оборудовании, принадлежащем Прокопьеву А.Н. при помощи сканера, принадлежащего Дайданову И.Ю. По делу изъяты системные блоки, принадлежащие Прокопьеву А.Н., Дайданову И.Ю., цветные принтеры, дискеты.

НА ИССЛЕДОВАНИЕ ПРЕДСТАВЛЕНЫ:

1. Системный блок компьютера, изъятый у Прокопьева А.Н.

ПЕРЕД ЭКСПЕРТОМ ПОСТАВЛЕНЫ ВОПРОСЫ:

Имеются ли на жестком диске представленного системного блока файлы, которые содержат изображения денежных купюр?

ИССЛЕДОВАНИЕ:

1. ВНЕШНИЙ ОСМОТР

Объект на экспертизу доставлен нарочным.

Системный блок компьютера представлен без упаковки. Лицевая и боковые стороны системного блока заклеены фрагментами прозрачной липкой ленты типа «скотч». Этими же фрагментами ленты прикреплен лист бумаги, закрывающий лицевую сторону системного блока, и два фрагмента бумаги с оттисками круглой печати «№9*УВД Курганской области*МВД Российской Федерации». На одном фрагменте бумаги имеются росписи. К верхней стороне системного блока фрагментами прозрачной бесцветной липкой ленты типа «скотч» прикреплен лист бумаги. На листе бумаги имеется пояснительный рукописный текст: «Системный блок, изъятый у Прокопьева А.Н.».

Системный блок представляет собой IBM совместимый компьютер конфигурации АТХ (см. Приложение, рис. 1).

Системный блок состоит из следующих комплектующих.

Таблица 1.

Комплектующие	**Марка (фирма-изготовитель)**	**Модель**	**Серийный номер**	**Примечание**
Системный (корпус)		Minitower ATX		Серийный номер блока питания 456578
Материнская плата	GIGABYTE P4 Titan533	GA-8IEX	0232002204	
Процессор	INTEL	CELERON 1.8GHZ	3226A475-1311	2 шт.
Модули памяти		M10718 PC2100 128Mb	На каждом имеется наклейка оранжевого цвета с маркировкой «52765048»	
Дисковод	MITSUMI	D359M3D	P4DM9080874	3,5"
Видеокарта	PalitDaytona	GEFORCE4 MX440 64MB TV-OUT	71ATO02029709	
Жесткий диск (НЖМД)	Seagate Barracuda ATA IV	ST340016A	3HS8EB3M	40 Гб

При включении представленного системного блока (без жесткого диска) установлено, что системные дата и время соответствуют текущим.

Для производства исследования использовалась стендовая ПЭВМ с процессором Intel Pentium III-1000 с тактовой частотой 1000 Мгц, ОЗУ 256 Мб и жестким диском 60 Гб. На стендовой ПЭВМ были установлены: операционная система (ОС) Windows 98 русская версия, программная оболочка Windows Commander версия 3.52, пакет программ Norton Utilities, пакет программ Microsoft Office, программа Kaspersky Anti Virus (AVP) версия 3.5.133.0, программа ADCSee32 версия 2.4, программа AVSearch v3.12a, CorelDRAW v9.337.

Для просмотра информации с жесткого диска представленного компьютера она предварительно копировалась на дополнительный жесткий диск стендовой ПЭВМ емкостью 6,5 Гб. Для восстановления удаленных файлов использовалась программа UnErase Wizard из пакета Norton Utilities. Следует отметить, что не все файлы, восстанавливаемые данной программой, пригодны к использованию. Поэтому рассматривались только восстановленные неповрежденные файлы, которые могли быть безошибочно использованы каким-либо имеющимся программным обеспечением на стендовой ПЭВМ. Удаленные файлы во избежание повреждения информации восстанавливались на диск стендового компьютера.

Исследуемый жесткий диск подключали к стендовому компьютеру в качестве дополнительного съемного диска. Работа по исследованию представленного НЖМД включала в себя общий осмотр жесткого диска, просмотр выявленных файлов, восстановление и просмотр удаленных файлов. Для просмотра каталогов и файлов с НЖМД исследуемого системного блока они предварительно копировались на диск стендового компьютера. В результате общего осмотра НЖМД установлены следующие признаки, которые сведены в таблицу 2.

Таблица 2.

Общие признаки исследуемого НЖМД

Объект	Емкость диска	Количество разделов	Имя раздела (диск в системе)	Емкость раздела (байт)	Файловая система	Занято (байт)	Каталогов (папок)	Файлов (всего)
НЖМД	40Гб	2	HARDC (C:)	10476945408	FAT32	9545441280	2115	41268
			HADR2 (D:)	29514285056	FAT32	25102516224	2109	33539

В результате осмотра НЖМД обнаружены файлы.

Таблица 3.

Файлы, содержащие информацию по уголовному делу, находящиеся на представленном НЖМД

№ п/п	Путь	Имя файла	Размер (в байтах), дата создания	Описание файла
1	D:\Рефераты\editors\рефффф\рефффф\	4.cdr	1105302 08.12.2002 15:35:12	Содержит графическое изображение оборотной стороны купюры достоинством 50 рублей. Файл распечатан из графического редактора CorelDRAW v9.337 на принтере фирмы EPSON модели EPSON STYLUS C62 (см. Приложение с. 4)
2	D:\Рефераты\editors\рефффф\рефффф\	5.cdr	1144538 08.12.2002 15:35:22	Содержит графическое изображение лицевой стороны купюры достоинством 50 рублей. Файл распечатан из графического редактора CorelDRAW v9.337 на принтере фирмы EPSON модели EPSON STYLUS C62 (см. Приложение с. 5)

При осмотре НЖМД, файлов, в удаленном виде содержащих графические изображения денежных купюр, не обнаружено.

ВЫВОД

На НЖМД системного блока, представленного на экспертизу, имеются файлы, содержащие графические изображения денежных купюр. Файлы описаны в таблице 3 заключения и распечатаны в Приложении к заключению эксперта (с. 4, 5).

Эксперт И.И.Иванов

Постановка вопроса эксперту представляется чрезмерно лаконичной. По уголовному делу подлежат доказыванию различные обстоятельства. Эксперт в состоянии не только установить факт наличия изображения денежной купюры на компьютере, но также сказать кое-что про следующие обстоятельства:

- когда это изображение было туда помещено;
- при помощи каких средств это изображение было изготовлено и/или обработано;
- когда оно было изготовлено;
- есть ли следы обработки, распечатки, копирования этого изображения.

Возможно, не на все перечисленные вопросы эксперт мог дать категоричный ответ. Возможно, на некоторые из них он ответил бы предположительно. Все равно такие ответы послужили бы к изобличению фальшивомонетчиков. Простое присутствие изображений денежных купюр на компьютере еще ни о чем не говорит. К примеру, на компьютере автора эти изображения также присутствовали, поскольку они были приложены к заключению эксперта, которое автор получил от своего корреспондента в электронном виде.

Судя по описанию компьютера, он был опечатан неправильно, то есть не опечатаны разъемы питания и подключения периферии. Если автор правильно понял написанное экспертом, то следует признать, что неизменность доказательств не была обеспечена. И этот факт добросовестный эксперт обязан был указать в своем заключении открытым текстом. Если же автор понял неправильно и разъемы компьютера все-таки были опечатаны, то следует отметить неясность в формулировках.

Эксперт вовсе не обязан подробно описывать внешний вид и состояние объекта исследования. Такое описание, конечно, не повредит. Однако оно не требуется. А вот что точно требуется для правильной оценки доказательств – это неизменность. Эксперт, по мнению автора, обязан отразить свое мнение по поводу сохранности и неизменности компьютерной информации на исследуемом объекте. Например, так: «состояние печатей свидетельствует, что доступ к содержащейся в компьютере информации был невозможен с момента изъятия до момента начала экспертизы».

Положительный пример

Далее приводится заключение, которое если и не идеально, то может служить образцом почти для всех российских экспертов.

Перед экспертом поставлены вопросы:

1) Имеются ли в памяти системного блока персонального компьютера, изъятого в НГКИ, файл, содержащий текстовый фрагмент согласно Приложению? Если данный файл имеется, то каково его месторасположение в памяти системного блока компьютера?

2) Какова дата создания данного файла?

3) Удалялся ли данный файл, если да, то какова дата его удаления?

4) Подлежит ли данный файл восстановлению, если да, то имеется ли возможность изготовить его копию на бумажном носителе?

Внешний осмотр поступивших объектов

Картонная коробка, заклеенная фрагментами бумаги, на поверхности которых имеются оттиски круглой печати: «УБОП при УВД ЯНАО*МВД РФ УПРАВЛЕНИЕ ПО БОРЬБЕ С ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ*ИНН 8901003107*ПРИ УПРАВЛЕНИИ ВНТРЕННИХ ДЕЛ ЯМАЛО-НЕНЕЦКОГО АО ЗОНАЛЬНЫЙ ОТДЕЛ г. НОЯБРЬСКА» и рукописный текст «ПОНЯТЫЕ 1 (подпись), 2 (подпись)». Целостность упаковки и оттисков печати видимых повреждений не имеет. При вскрытии упаковки извлечен системный блок в корпусе светло-серого цвета (металлик) типоразмера «MiddleTower» максимальными размерами 42,0Х18,0Х43,4 см (высота Х ширина Х длина). Лицевая декоративная накладка выполнена из пластмассы черного цвета.

Копия письма (представлена в Приложении к заключению эксперта).

ИССЛЕДОВАНИЕ

1. План исследования

1.1 Исследование системного блока производили в следующей последовательности:

– исследование состояния системного блока и определения его технических характеристик;

– исследование состояния накопителя (НЖМД) и определение его технических характеристик;

– исследование файловой системы и информации на НЖМД;

– исследование программного обеспечения на НЖМД;

– исследование компьютерной информации с целью поиска текстовых файлов;

– исследование компьютерной информации с целью поиска удаленных файлов и их последующего восстановления;

– исследование компьютерной информации с целью поиска программного обеспечения для защиты информации и поиск файлов, защищенных при помощи данного программного обеспечения.

2. Методика исследования

2.1. Исследование системного блока производили по следующей методике:

Исследование состояния системного блока проводилось по следующей методике:

– производилось вскрытие корпуса системного блока;

– визуальным осмотром устанавливался состав внутренних аппаратных компонентов (комплектующих устройств) представленного на исследование системного блока;

– из системного блока извлекался НЖМД; процедура изъятия носителя данных обусловлена требованием полной сохранности исследуемой информации путем обеспечения условий, исключающих какую-либо запись на них новых данных;

– к системному блоку в соответствии с эксплуатационными правилами подключались электропитание, монитор и клавиатура;

– системный блок включался, производилась загрузка операционной системы с системной дискеты эксперта, определение установленной системной даты и времени, диагностирование входящих в системный блок устройств.

Исследование состояния НЖМД (установленного в системном блоке) проводилось последовательно по следующей методике:

– визуальным осмотром устанавливался интерфейс, состояние перемычек и переключателей НЖМД;

– исследуемый НЖМД помещался в стендовую ПЭВМ; производилась загрузка операционной системы с загрузочного компакт-диска эксперта (сохранность данных на исследуемом НЖМД обеспечивалась утилитой PDBlock Lite фирмы Digital Intelligence Inc.) и программой partinfo.exe (из комплекта PowerQuest Partition Magic 8.0), определялись технические параметры НЖМД (количество цилиндров, сторон (головок), секторов на треке, количество секторов, размеров секторов и емкости);

– выявлялись таблицы разделов НЖМД с определением их основных параметров (начало и конец раздела, тип файловой системы, идентификаторы и метки разделов);

– определялась логическая адресация системных областей разделов НЖМД (загрузочной записи, главной файловой таблицы MFT, корневого каталога);

– производился поиск признаков повреждения целостности структуры данных (несоответствие заявленных параметров раздела фактическим, наличие сбойных, потерянных кластеров) и устанавливалась возможность доступа к данным на исследуемом НЖМД;

– исследуемый НЖМД помещался во внешний корпус для быстрой смены НЖМД, подключался к лабораторному компьютеру по USB-порту (сохранность данных на исследуемом НЖМД обеспечивалась программой NCSF Software Write-block XP организации National Center For Forensic Science);

– производилось создание файла-образа, содержащего точную копию исследуемого НЖМД на вспомогательном НЖМД лабораторного компьютера путем посекторного копирования с фиксацией технических параметров формата носителя с использованием специального программного обеспечения для экспертного исследования компьютерных носителей информации;

– осуществлялся вывод в файл на НЖМД лабораторного компьютера списка всех папок (каталогов) и файлов логических дисков исследуемого НЖМД.

Исследование файловой системы и информации на НЖМД системного блока, поступившего на экспертизу, проводилось по следующей методике:

– производился поиск файлов с расширением имен, соответствующих программам-архиваторам; выявленные архивные файлы разархивировались в отдельную папку (каталог) на НЖМД лабораторного компьютера;

– производился поиск удаленных файлов; файлы, подлежащие восстановлению, восстанавливались в отдельную папку (каталог) НЖМД лабораторного компьютера;

– производился поиск скрытых (зашифрованных) данных (логических и виртуальных дисков, папок (каталогов) и файлов данных);

– определялись признаки поиска информации (ключевые слова, изображения, расширения имен файлов и т.д.), соответствующие задачам исследования;

– производился поиск файлов, содержащих искомые признаки, с помощью специальных программ поиска информации на исследуемом носителе данных (точной копии) и в каталогах с восстановленными и разархивированными файлами на лабораторном компьютере;

– осуществлялся просмотр (визуализация) выявленных файлов, содержащих искомые признаки с помощью соответствующего программного обеспечения;

– производилась распечатка информации из файлов, содержание которых соответствует задачам исследования.

3. Экспертное оборудование и методическая литература, использованные при проведении исследования

3.1. Аппаратно-программный комплекс для экспертного исследования компьютерных носителей информации в составе:

– персональная ЭВМ на базе процессора AMD Athlon XP-M 3000+ производства фирмы «MEDION» (Германия);

– лазерный принтер «HP LaserJet 1200» производства «Hewlett Packard» (США);

– внешний корпус для быстрой смены НЖМД модель USB2.0-HDD3-EUR-1;

– программное обеспечение для экспертного исследования компьютерных носителей информации «EnCase Forensic Edition v.4.20» производства «Guidance Software Inc.» (США);

– операционная система «Microsoft Windows XP Home Edition» производства «Microsoft» (США);

– прикладное программное обеспечение «Microsoft Word» производства «Microsoft» (США);

– антивирусное программное обеспечение «eTrust Antivirus v.7.1.192» фирмы «Computer Associates International Inc.»;

– сервисное программное обеспечение «PDBlock Lite» фирмы «Digital Intelligence Inc.»;

– сервисное программное обеспечение «NCSF Software Write-block XP» организации «National Center For Forensic Science»;

– сервисное программное обеспечение «Partition Magic 8.0» фирмы «PowerQuest».

3.2. Методическая и справочная литература:

Зубаха В.С., Саенко Г.В., Усов А.И. и др. Общие положения по назначению и производству компьютерно-технической экспертизы: Методические рекомендации. – М.: ГУ ЭКЦ МВД России, 2001;

Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. М., 2001;

Усов А.И. Методы и средства решения задач компьютерно-технической экспертизы: Учебное пособие. – М.: ГУ ЭКЦ МВД России, 2002;

Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: Учебное пособие / А.И.Усов // Под ред. проф. Е.Р.Россинской. М., 2003;

EnCase Forensic Edition v.4. Руководство пользователя. Guidance Software, 2003;

Тушканова О.В. Терминологический справочник судебной компьютерной экспертизы: Справочное пособие. – М.: ГУ ЭКЦ МВД России, 2005.

4. Результаты исследования

4.1. Исследование системного блока:

Визуальным осмотром установлено, что корпус системного блока, представленного на экспертизу, внешних повреждений не имеет. Правая боковая сторона системного блока опечатана двумя бумажными пломбами с №№007574, 007573. Представленный системный блок состоит из следующих комплектующих:

Таблица 1.

Комплектующие, входящие в состав системного блока

Комплектующие	**Фирма изготовитель Марка**	**Модель**	**Серийный номер**	**Примечание**
Блок питания		200X		
Материнская плата	ASUS	PSLD2-VM	5AM0AB050239	
Процессор	INTEL		Серийный номер на вентиляторе 5622D	Не извлекался в связи с высокой вероятностью повреждения
Модуль памяти	GEIL	512MB PC2-4300 DDR2-533	GX25124300X	
Дисковод (НГМД)	NEC	FD1231H	JAPL58JC0026	
НЖМД Barracuda	Seagate, НЖМД	ST3160812AS	5LS06CZY обозначение –	Эксперт вводит 7200.7
Привод компакт-дисков	NEC Corporation	ND-4550A	5XC9R92S111	

Для последующего исследования на стендовом экспертном оборудовании произведено изъятие из системного блока указанного НЖМД.

В результате исследования состояния системного блока, без НЖМД, установлено:

– значение системной даты, имеющееся в BIOS представленного на исследование системного блока, соответствует текущей;

– значение системного времени, имеющееся в BIOS представленного на исследование системного блока, соответствует текущему.

Исследование информации на НЖМД.

Исследование состояния накопителя на жестких магнитных дисках (НЖМД).

Исследуемый НЖМД помещался в стендовую ПЭВМ; производилась загрузка операционной системы с загрузочного компакт-диска эксперта (сохранность данных на исследуемом НЖМД обеспечивалась утилитой PDBlock Lite фирмы Digital Intelligence Inc.) и программой partinfo.exe (из комплекта PowerQuest Partition Magic 8.0), определялись технические параметры НЖМД (количество цилиндров, сторон (головок), секторов на треке, количество секторов, размеров секторов и емкости);

– выявлялись таблицы разделов НЖМД с определением их основных параметров (начало и конец раздела, тип файловой системы, идентификаторы и метки разделов, размер и количество кластеров);

– определялась логическая адресация системных областей разделов НЖМД (загрузочной записи, главной файловой таблицы MFT, корневого каталога).

В результате исследования установлены следующие параметры исследуемого НЖМД:

Таблица 2.

№ п/п	Значения параметров НЖМД			
	Количество цилиндров в системе адресации CHS	**Количество головок в системе адресации CHS**	**Количество секторов на дорожке в системе адресации CHS**	**Значение хэш–функции, рассчитанное для НЖМД по алгоритму MD5**
НЖМД	19457	255	16	C7124548E12795B9C15BCEEE1BDF10E9

Исследуемый НЖМД имеет параметры разделов, приведенные в таблицах №№3, 4.

Таблица 3.

№ п/п	Раздел	Тип раздела	Начало раздела			Конец раздела		
			Цилиндр	**Сторона**	**Сектор**	**Цилиндр**	**Сторона**	**Сектор**
НЖМД	№1 (C:)	NTFS	0	1	1	5098	254	63
		Extended	5099	0	1	16708	254	63
	№2 (D:)	NTFS	5099	1	1	16708	254	63
	Неразмеченная область		16709	0	1	19456	254	63

Таблица 4.

№ п/п	Раздел	Формат раздела	Номер раздела	Метка раздела	Объем раздела (байт)	Занято (байт)
НЖМД	№1 (C:)	NTFS	183ED056		41940669952	3829933568
	№2 (D:)	NTFS	942AB287		95495468032	70546432

Исследуемый НЖМД не имеет повреждений целостности структуры данных, доступ к данным возможен.

Исследование файловой системы и информации на НЖМД.

Исследуемый НЖМД подключали к лабораторному компьютеру в качестве внешнего съемного диска по USB-шине. Исследуемый НЖМД защищали от записи с помощью программного средства блокирования записи NTFS Software Write-block XP (блокиратора записи, разработанного National Center For Forensic Science). Исследование файловой системы и информации, содержащейся на НЖМД, проводилось на точной копии (образе) исследуемого накопителя, созданного на лабораторном компьютере с помощью программного обеспечения для экспертного исследования компьютерных носителей информации EnCase Forensic Edition v.4.20, а также в каталогах с восстановленными и разархивированными файлами на лабораторном компьютере.

Исследованием установлено, что на НЖМД имеются удаленные и подлежащие восстановлению файлы. Восстановление удаленной информации произведено при помощи программного обеспечения для экспертного исследования компьютерных носителей информации EnCase Forensic Edition v.4.20 в отдельную папку (каталог) на лабораторном компьютере.

Исследованием установлено, что на НЖМД имеются файлы с расширением имен, соответствующих программам-архиваторам, которые содержат архивные файлы. Разархивация выявленной информации произведена в отдельную папку (каталог) на лабораторном компьютере.

На НЖМД с помощью программного обеспечения для экспертного исследования компьютерных носителей информации EnCase Forensic Edition v.4.20 произведен контекстный поиск информации, соответствующей задаче исследования. В результате проведенного поиска обнаружены файлы, содержащие данные, соответствующие задаче исследования. Обнаруженные файлы описаны в таблице.

Таблица 5.

Файлы, обнаруженные на НЖМД

№ п/п	Накопитель	Путь	Имя файла	Размер (байт)	Примечание
1	НЖМД	C\RECYCLER\S-1-5-21-1456376166-2215607188-3175822896-1614\	Dc5835.doc	21504	Файл распечатан, с. 12
2	НЖМД	C\RECYCLER\S-1-5-21-1456376166-2215607188-3175822896-1614\	Dc5780.tmp	21504	Файл распечатан, с. 13

Кроме того, в свободной области НЖМД (в области, не относящейся к конкретному файлу файловой системы) в секторах 30761049594-30761051724 и 30762325498-30762327628 обнаружена информация, аутентичная содержанию копии письма, которая распечатана на с. 10, 11.

Обнаруженные файлы являются удаленными файлами. Определить время удаления файлов не представляется возможным, так как файловая система в данном случае не сохранила подобную служебную информацию. На основе анализа данных, находящихся в $MFT НЖМД, представленного на исследование, установлено, что удаленный файл Dc5835.doc имел имя файла в файловой системе «Письмо Петрову.doc"

Анализом метаданных обнаруженных файлов установлено:
Файл **Dc5835.doc** содержит в метаданных следующие сведения:
Создан: 02.09.2004 11:37:00
Изменен (дата последнего сохранения): 13.09.2005 18:21:00
Напечатан (последний раз): 01.10.2004 13:45:00

Автор: IVANOVA
Организация: OFFICE
Редакция: 3
Общее время правки (в минутах): 63

Авторы последних 10 изменений:

Таблица 6.

Автор	**Путь**
IVANOVA	C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\Автокопия Документ1.asd
IVANOVA	C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc
IVANOVA	C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\Автокопия Письмо Петрову.asd
IVANOVA	C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc
IVANOVA	C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc

Файл Dc5780.tmp содержит в метаданных следующие сведения:
Создан: 02.09.2004 11:37:00
Изменен (дата последнего сохранения): 13.09.2005 18:21:00
Напечатан (последний раз): 01.10.2004 13:45:00

Автор: IVANOVA
Организация: OFFICE
Редакция: 3
Общее время правки (в минутах): 63
Авторы последних 10 изменений:

Таблица 7.

Автор	**Путь**
IVANOVA	C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\Автокопия Документ1.asd
IVANOVA	C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc
IVANOVA	C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\Автокопия Письмо Петрову.asd
IVANOVA	C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc
IVANOVA	C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc

ВЫВОДЫ:

1-4. На НЖМД системного блока, представленного на экспертизу, обнаружен удаленный файл Dc5835.doc, содержание которого аутентично копии письма, представленного на экспертизу. Файл описан в таблице 5 заключения эксперта и распечатан на с. 12. На основе анализа метаданных данного файла установлено, что он был создан 02.09.2004 11:37:00 пользователем IVANOVA, организация OFFICE (по сведениям, содержащимся в файле Dc5835.doc); изменен (дата последнего сохранения): 13.09.2005 18:21:00; напечатан (последний раз): 01.10.2004 13:45:00. Пользователем системного блока, представленного на экспертизу, согласно данным, имеющимся в файловой системе исследованного НЖМД, является VETROVA.

Копии данного файла могут находиться на НЖМД системного блока

Автор	**Путь**
Автокопия Документ1.asd	C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\
Письмо Петрову.doc	C:\Documents and Settings\IVANOVA\Мои документы\письма\
Автокопия Письмо Петрову.asd	C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\

пользователя IVANOVA по следующим координатам:

На основе анализа данных, находящихся в $MFT НЖМД, представленного на экспертизу, установлено, что удаленный файл Dc5835.doc имел имя файла в файловой системе «Письмо Петрову.doc». Определить время удаления файла Dc5835.doc не представляется возможным по причинам, указанным в исследовательской части заключения.

На представленном НЖМД обнаружен удаленный файл Dc5780.tmp, который, вероятно, является временной копией файла Dc5835.doc. Файл описан в таблице 5 заключения эксперта и распечатан на с. 13.

В свободной области НЖМД (в области, не относящейся к конкретному файлу файловой системы) системного блока, представленного на экспертизу, в секторах 30761049594-30761051724 и 30762325498-30762327628 обнаружена информация, аутентичная содержанию копии представленного письма. Обнаруженная информация распечатана на с. 10, 11.

Постановка вопросов перед экспертом предельно корректна. Следователь избегает скрытых утверждений и не требует от эксперта установления нетехнических фактов, например, кем было написано письмо. В то же время следователь не ограничивается вопросом о наличии информации на диске. Он также интересуется обстоятельствами ее появления и расположения. Как уже отмечалось ранее, само по себе наличие информации на НЖМД еще ни о чем не свидетельствует – информация могла попасть на диск несколькими различными путями, в том числе без ведома и желания последнего владельца исследуемого компьютера.

Следует отметить грамотное применение экспертом специальных технических средств – стендовой ЭВМ со специальной экспертной ОС, блокиратора записи на исследуемый диск, экспертной программы «EnCase».

Из недостатков этого заключения автор может указать разве что некоторый избыток технических деталей и употребление непонятных для судьи терминов типа «таблица MFT» или «USB-шина», без которых можно было бы обойтись. Обилие технической терминологии может запутать неспециалиста и вызвать претензии защиты по поводу языка, на котором составлен документ, или по поводу разъяснения сути обвинений.

6. Участие специалиста в судебном заседании

УПК предусматривает участие специалиста как при проведении следственных действий, так и в судебном заседании. Но в следственных действиях специалист участвует часто, а в суде – редко. По компьютерным же преступлениям участие специалиста требуется значительно чаще. В следственных действиях – всегда, а в судебном заседании – относительно часто. Почему? Ответ очевиден: потому что обилие специальных терминов и специфических компьютерных сущностей делают документы, справки, показания свидетелей малопонятными для неподготовленных людей. И специальные знания требуются буквально на каждом шагу.

В ходе судебного заседания по сложным компьютерным преступлениям специалист действует как своеобразный переводчик с профессионального языка на общечеловеческий (в идеале – на юридический).

Беда лишь в том, что такой «перевод» не всегда возможен. Объяснить значение компьютерного термина невозможно без объяснения сущности, которую этот термин называет. А для объяснения сущности требуется объяснить несколько других сущностей и так далее.

Непонимание участниками процесса специфических терминов (использование которых неизбежно как в обвинительном заключении, так и в свидетельских показаниях) ведет к неверному пониманию обстоятельств дела и даже сути совершенных деяний. Это непонимание нередко используется для введения суда в заблуждение стороной обвинения или стороной защиты.

Каждый раз, когда автору приходится участвовать в судебном процессе – будь то процесс гражданский или уголовный, – он вспоминает сцену из знаменитого романа Леонида Соловьева.

– Может быть, мой почтенный и мудрый собрат несравненно превосходит меня в какой-либо другой области познаний, но что касается звезд, то он обнаруживает своими словами полное незнакомство с учением мудрейшего из всех мудрых ибн-Баджжа, который утверждает, что планета Марс, имея дом в созвездии Овна и Скорпиона, возвышение в созвездии Козерога, падение в созвездии Рака и ущерб в созвездии Весов, тем не менее всегда присуща только дню вторнику, на который и оказывает свое влияние, пагубное для носящих короны.

Отвечая, Ходжа Насреддин ничуть не опасался быть уличенным в невежестве, ибо отлично знал, что в таких спорах побеждает всегда тот, у кого лучше привешен язык. А в этом с Ходжой Насреддином трудно было сравниться.

Л.Соловьев. Повесть о Ходже Насреддине

Жонглируя малопонятными техническими терминами, языкастый адвокат легко создаст впечатление, что он прав, а эксперт, напротив, некомпетентен в своей области. Бывает и наоборот.

Вот почему автор настойчиво рекомендует приглашать для участия в судебных заседаниях независимого специалиста. И в ходе заседания велеть ему разъяснять все специфические термины и сущности.

К большому сожалению, специалист если и приглашается, то какой-то одной стороной. Как правило, это сторона защиты или потерпевшая сторона. В таких условиях специалист воспринимается судом как «специалист стороны», то есть его мнению априорно приписывается тенденциозность. И противная сторона воспринимает специалиста так же и пытается его дискредитировать, оспорить мнение, найти основание для отвода. Хотя УПК предусматривает, что специалист должен быть независим.

Автор рекомендует в тех случаях, когда это возможно, заранее согласовывать кандидатуру специалиста между сторонами.

7. Тенденции и перспективы

Тенденции

Для чего специалисту нужно иметь представление о текущих тенденциях отрасли ИТ в целом и высокотехнологичной преступности в частности? Для того чтобы не пойти по ложному пути, впервые столкнувшись с чем-то принципиально новым, до того не известным. А новое в нашей отрасли возникает значительно чаще, чем в какой-либо другой. Возьмем, например, кросплатформенные вирусы. До сего момента известен лишь один образец такого вируса (Cxover), к тому же не получивший распространения. Но появление следующих образцов – лишь вопрос времени. Столкнувшись с труднообъяснимым фактом, специалист или эксперт-криминалист должен вспомнить о такой тенденции и сделать предположение, что появился кросплатформенный вирус. То есть для раскрытия и расследования компьютерных преступлений наряду с опытом (своим и чужим) специалистам должна помогать также экстраполяция текущих тенденций.

Развитие форензики в 2005-2006 годы характеризовалось следующими тенденциями:

- Выделение технических систем для сбора и хранения цифровых доказательств из систем защиты информации. Всевозможные логи, архивные копии, копии переписки и иных сообщений собираются и хранятся именно с целью расследования будущих возможных инцидентов, а не с целью восстановления на случай утраты (копии для случаев утраты делаются отдельно). Например, в политике безопасности некоторых компаний предусмотрено, что после увольнения любого сотрудника делается полная копия НЖМД его служебного компьютера, которая хранится в течение достаточного времени на случай возможных расследований.
- Дальнейшее совершенствование систем для снятия информации с цифровых каналов связи (СОРМ), их повсеместное внедрение. Ведущие производители коммуникационного оборудования объявили о внедрении функций «lawful interception» непосредственно в аппаратную часть своего оборудования и во встроенное ПО, чтобы операторы связи, с которых государственные органы требуют наличия таких возможностей, не тратились на отдельное оборудование для перехвата [78].

```
Пример конфигурации маршрутизатора (Cisco IOS 12.2) для включения доступа к
функции перехвата трафика:

Router(config)# snmp-server view tapV ciscoTap2MIB included
Router(config)# snmp-server view tapV ciscoIpTapMIB included
```

```
Router(config)# snmp-server view tapV ciscoTap802MIB included
Router(config)# snmp-server view tapV ciscoTapConnectionMIB included
Router(config)# snmp-server group tapGrp v3 noauth read tapV write tapV
notify tapV
Router(config)# snmp-server user ss8user tapGrp v3 auth md5 ss8passwd
Router(config)# snmp-server engineID local 1234
```

- Возникновение компьютерно-криминалистических (или аналогичных) подразделений как в правоохранительных органах, так и в корпоративных службах информационной безопасности. Речь идет не о создании «компьютерной полиции», которая появилась еще в 1990-е, а именно о выделении криминалистических подразделений из состава этой полиции или корпоративных департаментов информационной безопасности. Об отделении задач сбора цифровых следов и задач расследования. Об отделении задач защиты информационных систем и задач по расследованию инцидентов.
- Появление кафедр и иных научных подразделений, специализирующихся на компьютерной криминалистике. То есть эта наука выделилась не только методически, но и организационно.

Теперь разберем долговременные тенденции, относящиеся к рассматриваемой науке.

Понимание и просвещение

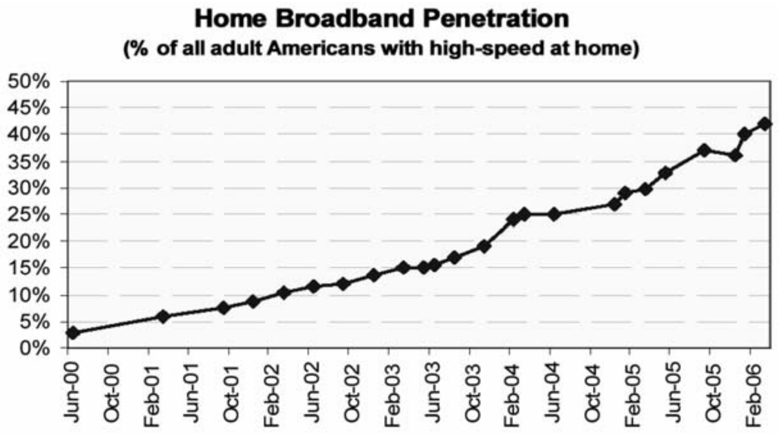
Как уже отмечалось выше, для следователей, прокуроров и судей описания преступных действий подозреваемого (обвиняемого) в компьютерном преступлении могут оказаться просто непонятными. Невозможно объяснить, каким именно способом злоумышленник получил несанкционированный доступ к серверу через сеть, не объяснив предварительно, что такое сервер, удаленный доступ и как работает сеть. А объяснить все это невозможно без других знаний из области ИТ. Автор неоднократно сталкивался с ситуацией, когда показания и объяснения эксперта в суде из всех присутствующих понимает только один человек – подсудимый.

С другой стороны, пользователи и технические специалисты в массе своей остаются непросвещенными относительно правовых вопросов. В их среде часто бытуют довольно странные представления о законе и законности, которые, похоже, основаны на просмотре голливудских боевиков. Например, системные администраторы часто на полном серьезе утверждают, что «правила использования информационного ресурса определяются владельцем этого ресурса и никем иным».

Таким образом, существует пропасть непонимания между юристами и техническими специалистами. Преодолеть ее при помощи просвещения вряд ли удастся. Повышение так называемой «компьютерной грамотности» юристов и объяснение технарям основ законодательства – это, безусловно, дело полезное. Но обе упомянутые области настолько сложны и обширны, что нет никакой надежды совместить профессиональные юридические и профессиональные компьютерные знания для сколь-нибудь значительной группы людей. Специалистов, способных переводить с «технического» на «юридический» и обратно, свободно владеющих обоими языками, довольно мало. Поэтому проблемы с пониманием и с правовой оценкой действий в киберпространстве – останутся.

Широкополосный доступ

Дешевый широкополосный доступ в Интернет для частных (домашних) пользователей начал предоставляться в массовых масштабах в развитых странах в 2000 2001 годах. Чуть позже такой доступ появился в других странах. В России широкополосный доступ для домашних пользователей стал обычным делом в Москве в 2005 году, а в областных центрах он будет внедрен в 2008-2009 годах. То есть можно сказать, что домашний пользователь на широком канале – это массовое явление, в том числе и в нашей стране.



Процент граждан США, имеющих дома широкополосный доступ в Интернет. Источник – [79]

Широкополосный доступ выглядит крайне привлекательно, с точки зрения киберпреступников. Домашние пользователи не в состоянии защитить свои компьютеры от внедрения вредоносных программ. В отличие от корпоративных компьютеров, здесь отсутствуют какие-либо дополнительные средства защиты информации – сервера доступа с трансляцией адресов, межсетевые экраны, системы обнаружения атак. Можно быть уверенным, что из нескольких миллионов таких компьютеров нес-

колько десятков тысяч наверняка обладают определенной уязвимостью. Именно на них основываются зомби-сети. Компьютеры с медленным, коммутируемым соединением для зомбирования малополезны.

Распространение широкополосного доступа дало новый толчок технологиям рассылки спама. Если в 2002 году бóльшая часть спама рассылалась через плохо защищенные сервера электронной почты и собственные сервера спамеров, то уже с 2004 года статистика однозначно свидетельствует, что бóльшая часть спама рассылается через затрояненные компьютеры на быстрых каналах связи.

Персональные компьютеры, обслуживаемые неквалифицированными пользователями и подключенные к широкополосным линиям связи, будут в дальнейшем только множиться. Значит, на этом ресурсе будут основаны многие технологии злоумышленников – рассылка спама, DoS-атаки, хостинг нелегальных материалов, методы анонимизации, кража персональных данных и т.п.

Поскольку услуги связи постоянно дешевеют, внедряются новые, более производительные технологии и протоколы (например, Wi-Max), а тарифы используются преимущественно безлимитные, то пользователи не очень заинтересованы заботиться о защищенности своих компьютеров. Современные троянские программы не загружают ресурсы компьютера, используют имеющуюся полосу линии связи аккуратно, чтобы как можно дольше не обнаруживать своего присутствия. То есть пользователь зараженного компьютера не испытывает никаких явных неудобств от присутствия троянской программы. Неудобства от этого испытывает весь остальной мир. В аналогичной ситуации находится интернет-провайдер зараженного пользователя: он не несет прямых убытков, когда вредоносные программы функционируют в его сети, однако заинтересован, чтобы в сетях иных провайдеров вредоносных программ не было. Это создает основу для заключения многосторонних соглашений между операторами связи или объединения их под эгидой государства для совместной борьбы, взаимодействия и оказания взаимной помощи.

Подобные альянсы появляются постоянно. Из событий последних двух лет стоит отметить появление объединения операторов «Networks Fingerprint Sharing Alliance» для борьбы с DoS-атаками на основе продукта «Arbor Peakflow» [W26].

Интеллектуальная собственность

Повышение роли интеллектуальной собственности выражается в увеличении доли нематериальных вложений в стоимости почти всех видов продукции. Следовательно, и доходы производителя все больше и больше зависят от стоимости прав интеллектуальной собственности, которые он использует в производстве или которые продает. От величины этой стоимости существенным образом зависит стабильность экономики государств, где расположены крупнейшие правообладатели и производители «творческой» продукции. Размер стоимости авторских и патентных прав в товарообороте развитых стран таков, что сильные колебания этой стоимости могут привести к краху экономики. А стоимость интеллектуальной собственности поддерживается соответствующим законодательством и практическими мерами по его исполнению – то есть не рыночным, а административным механизмом. Понятно, что государство придает большое значение поддержанию стоимости нематериальных активов. Установление выгодных правил в области торговли интеллектуальной собственностью – одна из приоритетных задач внешней политики развитых стран.

Тенденция прослеживается достаточно четкая: постепенное увеличение объема полномочий правообладателя, расширение круга ценностей, на которые распространяются права интеллектуальной собственности, удлинение сроков охраны.

В то же время компьютерные технологии сделали необычайно легким отчуждение произведения от его носителя. Копирование и передача объектов интеллектуальной собственности в цифровой форме имеют ничтожную себестоимость и доступны практически всем. Это способствует легкости нарушения прав и затрудняет борьбу с такими нарушениями.

Ожидается продолжение данной тенденции в ближайшие годы.

То есть специалистам в области компьютерных преступлений следует ожидать усиления борьбы с нарушениями авторских прав, патентных прав, прав на товарные знаки и иных прав интеллектуальной собственности на цифровой контент. Наказания за соответствующие нарушения будут ужесточаться. Круг преступных деяний, скорее всего, расширится, поскольку, когда затруднительно пресекать сами нарушения (воспроизведение, например), пытаются запрещать то, что способствует таким нарушениям (например, файлообменные сети). На борьбу именно с правонарушениями в области интеллектуальной собственности надо ожидать наибольших ассигнований со стороны правообладателей и правительств заинтересованных стран.

С другой стороны, неизбежно и усиление реакции на подобные действия со стороны оппозиции, либералов, правозащитников, а также со стороны тех стран, которые являются потребителями и не являются производителями продуктов интеллектуальной собственности. Следует ожидать дальнейшей политизации борьбы с нарушениями авторских прав.

Конвергенция

Важной тенденцией развития отрасли связи является конвергенция различных сервисов и служб. По сетям с коммутацией пакетов (прежде всего – IP-сетям) ныне передаются не только данные, но и голос, видео-

изображение, управляющие сигналы для разнообразного оборудования, другие виды информации. По одному и тому же кабелю, по одному и тому же протоколу сетевого уровня в дом к потребителю подаются различные сервисы: телефонная связь, сигнал телевещания, видео по требованию, управление внешними устройствами и доступ в Интернет. Такая конвергенция упрощает и удешевляет все сервисы, хотя и делает их менее надежными, создавая единую «точку отказа». Впрочем, дублирование каналов эту проблему решает.

Эта тенденция порождает новые угрозы. Захват злоумышленником контроля над каналом передачи данных будет угрожать не только перехватом интернет-трафика, но и голосовой информации потребителя, а также сигналов управления бытовой техникой, охранными системами. То есть расширяется круг компьютерных преступлений.

Перспективы

Направления дальнейшего развития форензики на ближайшие годы видятся автору такими.

Законодательство

На взгляд автора, не стоит ожидать в ближайшие годы внесения таких изменений в законодательство, которые бы установили применение некоторых методов снятия и закрепления цифровых доказательств. С одной стороны, существующих методов, в принципе, достаточно. С другой стороны, степень компьютеризации нашего общества еще слишком незначительна; для существенных изменений нужно подождать смены одного поколения. Кроме того, следует учитывать скорость развития информационных технологий. Никакое законодательство не способно изменяться столь же быстро.

Криминалистическая техника

Что касается программ и аппаратных устройств для снятия информации с разнообразных носителей и ее исследования, то в этой области прорывов ожидать не стоит. Почти все, что можно было автоматизировать, уже автоматизировали. Развитие пойдет лишь по пути учета новых видов носителей и новых форматов данных.

Слежка

Многие считают, что в ближайшие годы будет падать эффективность систем перехвата коммуникаций (СОРМ, «Carnivore», «Echelon» и др.) вследствие все большей распространенности дешевых систем и протоколов шифрования, встраивания таких систем в различное ПО. Для многих

протоколов появляются их шифрованные версии (модификации, расширения). Широко доступны как описания, так и готовые реализации стойких алгоритмов шифрования, в том числе под свободными лицензиями. Мощность современных компьютеров такова, что шифрование в реальном времени любого разумного объема трафика занимает весьма незначительную часть ресурсов.

Национальное законодательство во многих случаях ограничивает применение шифрования или требует депонировать ключи, но любой пользователь без особого труда приобретает услуги зарубежного провайдера, где ограничения национального законодательства не действуют. Перечисленные факторы подтверждают, что среднему пользователю становится все легче защитить свои коммуникации от перехвата. Следовательно, желающих сделать это становится все больше.

Новые отношения

Как отмечалось в первом разделе книги, технический прогресс способствует возникновению новых видов преступлений двумя основными путями. Во-первых, непосредственно. Вновь появившиеся технические средства и технологии используются злоумышленниками для более эффективного совершения преступлений традиционных видов. Во-вторых, опосредованно. Технический прогресс вызывает прогресс социальный, то есть возникновение принципиально новых видов общественных отношений. Новые отношения означают новые права, которые могут быть нарушены. Таким образом, возникают принципиально новые виды преступлений, которые были раньше не то чтобы неосуществимы, но попросту немыслимы.

Среди принципиально новых общественных отношений, которые только что возникли или возникнут в ближайшие годы, следует отметить следующие:

- отношения по поводу прав на доменные имена и, возможно, некоторые другие средства индивидуализации в глобальных сетях;
- отношения по поводу виртуальных предметов, персонажей, недвижимости и иных активов, существующих в виртуальных мирах;
- отношения по поводу рекламных возможностей и иного влияния на людей различных сетевых ресурсов – веб-сайтов, блогов, сетевых сервисов, поисковых систем и т.п.;
- отношения по поводу прав интеллектуальной собственности на результаты работы отдельных программ и комплексов программ, в том числе комплексов независимых друг от друга программ;
- отношения по поводу технических стандартов, форматов и протоколов, которые формально являются добровольными, но фактически обязательны для всех и вследствие этого служат механизмом недобросовестной конкуренции;

- отношения по поводу новых видов использования интеллектуальной собственности.

При возникновении новых общественных отношений первое время они законом не защищаются. Но достаточно быстро общество осознает необходимость защиты новых прав, особенно в тех случаях, когда эти права начинают стоить существенных денег. До принятия новых законов, охраняющих новые права, многие юристы пытаются «натянуть» на них прежние нормативные акты. Иногда это удается, а порой возникают забавные или трагические казусы. Новейшая история показывает, что от момента возникновения нового общественного отношения до момента, когда возникнет более-менее единообразная юридическая практика его защиты, проходит от 5 до 8 лет.

Неолиберализм и неоконсерватизм

В постиндустриальных странах классический либерализм XIX-XX веков почти повсеместно сменен на новую политико-эконономическую доктрину, именуемую неолиберализмом [76, 77]. Неолиберализм характеризуется следующими тенденциями:

- сокращение реального влияния государства на общество;
- расширение роли так называемого гражданского общества;
- увеличение числа социальных иерархий;
- дерегуляция рынков, снятие ограничений на концентрацию капитала;
- транснациональное движение капитала, увеличение международного разделения труда;
- размывание понятия государственной и национальной принадлежности (космополитизм), кризис идентичности.

Как видно, Интернет воплощает в себе основные тенденции неолиберализма. Он принципиально трансграничен. Он трудно контролируем со стороны государства. Он почти не нуждается в централизованном управлении. Интернет пришелся как нельзя кстати неолиберальному обществу. И, напротив, для тех государств, которые не успели еще перейти к неолиберализму и задержались на предыдущей стадии развития (так называемые тоталитарные или просто патерналистские государства), наличие Интернета создает проблемы в идеологической сфере.

Неоконсерватизм уравновешивает недостатки неолиберализма и компенсирует кризис идентичности, позволяя сохранить единство государства при новом типе общества. Для неоконсерватизма характерны конфессионально-культурное объединение, насаждение толерантности, избрание общенационального врага (внешнего и внутреннего), который бы смог идеологически объединить такое космополитичное и мультикультурное общество.

Чем же уравновешиваются неолиберальные тенденции в Сети? Что является воплощением неоконсерватизма в Интернете?

Во-первых, борьба со «всенародным», то есть общецивилизационным врагом. На замену исчезнувшему социализму были подобраны другие враги – мировой терроризм (внешний), экстремисты (внутренний) и педофилы (внутренний). Для людей, крепко связанных с Интернетом, имеется и еще один объединяющий враг – спамеры.

Ведение борьбы с общими врагами позволяет найти платформу для национального и государственного единения, сублимировать недовольство, загрузить работой многочисленные государственные и общественные учреждения. То есть уравновесить негативные следствия неолиберальной политики.

Противодействие в Сети перечисленным врагам не будет уделом профессионалов, как для других компьютерных преступлений. Террористы, экстремисты, педофилы и спамеры, а также им сочувствующие будут (и уже сейчас являются) общим противником для самых широких кругов общества. Правоохранительные органы, ведя борьбу с соответствующими правонарушениями, будут иметь дело с самой широкой «инициативой снизу», игнорировать которую – себе дороже.

Возрастание роли Интернета

Тенденция, описанная в главе «Конвергенция», обещает нам расширение роли сетей с коммутацией пакетов, прежде всего – сетей на протоколе IP. Как все сервисы переводятся на IP, так и все связанные с ними злоупотребления становятся компьютерными.

В ближайшие годы мы можем, например, столкнуться с квартирной кражей как компьютерным преступлением. Значительная доля систем охранной сигнализации и видеонаблюдения работает на протоколе IP и осуществляет передачу информации по публичной IP-сети. Соответственно, отключить такую систему или навязать ей ложные данные можно дистанционно, через Интернет, осуществив к ней несанкционированный доступ при помощи компьютера. В случае успешного доступа взломанная система сама сообщит вору, когда хозяев нет дома, в нужный момент разблокирует замки и прекратит видеозапись.

Камера наблюдения «D-Link Securicat Network DCS-G900». Использует беспроводную связь по протоколу Wi-Fi (IEEE 802.11g) как для передачи видеосигнала, так и для управления камерой. Из-за этого злоумышленник получает потенциальную возможность захватить управление камерой, не проникая на охраняемый объект

Литература

Офлайновые публикации

1. Carvey H. Windows Forensics and Incident Recovery, 2004.
2. Jones R. Internet Forensics, 2005.
3. Solomon M., Broom N., Barrett D. Computer Forensics Jumpstart, 2004.
4. Mohay G., Anderson A., Collie B., de Vel O., McKemmish R. Computer and Intrusion Forensics, 2003.
5. Caloyannides M.A. Privacy Protection and Computer Forensics (Second Edition). – «Artech House Publishers», 2004.
6. Casey E. Digital Evidence and Computer Crime (2nd Edition), 2004.
7. Good Practice Guide for computer based Electronic Evidence, (версия 3.0). Association of Chief Police Officers (ACPO). Великобритания, 2006.
8. Вехов В.Б., Илюшин Д.А., Попова В.В. Тактические особенности расследования преступлений в сфере компьютерной информации: Научно-практическое пособие. 2-е изд. – М.: ЛексЭст, 2004.
9. Завидов Б.Д. Обычное мошенничество и мошенничество в сфере высоких технологий. М., 2002.
10. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. Воронеж, 2001.
11. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response – Recommendations of the National Institute of Standards and Technology (NIST), Publ. 800-86. 2006.
12. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. акад. Б.П.Смагоринского. – М.: Право и Закон, 1996.
13. Войскунский А.Е. Психологические исследования феномена интернет-аддикции // 2 я Российская конференция по экологической психологии. Тезисы.
14. Гуманитарные исследования в Интернете. М., 2000.
15. Мир Интернет. 1999, №9.
16. Рабовский С.В. Социальные аспекты информатизации российского общества. М., 2001.
17. Митрохина Е. Информационные технологии, Интернет, интернет-зависимость // журнал «Наука, политика, предпринимательство». 2004, №1. С. 83.

18. Schneier B. Applied Cryptography. Protocols, Algorithms, and Source Code in C. «John Wiley & Sons, Inc», 1996.
19. Федотов Н.Н. DoS-атаки в Сети. Введение, текущая практика и прогноз // журнал «Документальная электросвязь». 2004, №13 (http://www.rtcomm.ru/about/press/pa/?id=429).
20. Фирсов Е.П. Расследование изготовления или сбыта поддельных денег или ценных бумаг, кредитных либо расчетных карт и иных платежных документов / Монография под науч. ред. д.ю.н. проф. Комисарова В.И. – М.: Юрлитинформ, 2004.
21. Середа С.А., Федотов Н.Н. Расширительное толкование терминов «вредоносная программа» и «неправомерный доступ». // Закон, июль, 2007, с. 191.
22. Daigle L. RFC-3912 «WHOIS Protocol Specification», 2004.
23. Dagon D., Gu G., Zou C., Grizzard J., Dwivedi S., Lee W., Lipton R. A Taxonomy of Botnets (http://www.math.tulane.edu/~tcsem/botnets/ndss_botax.pdf).
25. Серго А.Г. Доменные имена. – М.: Бестселлер, 2006.
26. Mockapetris P. RFC-1034 «Domain names – concepts and facilities», 1987.
27. Mockapetris P. RFC-1035 «Domain names – implementation and specification», 1987.
28. Стандарт RFC-3986 «Uniform Resource Identifier (URI): Generic Syntax».
29. Arends R., Austein R., Larson M., Massey D., Rose S. Стандарт RFC-4034 «Resource Records for the DNS Security Extensions», 2005.
30. Fielding R., Mogul J., Masinter L., etc. RFC-2616 «Hypertext Transfer Protocol – HTTP/1.1», 1999.
31. Resnick P. (editor) Стандарт RFC-2822 «Internet Message Format», 2001.
33. Rivest R. RFC-1321. «The MD5 Message-Digest Algorithm», 1992.
34. NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995.
35. Schneier B. Cyberwar // Crypto-Gram Newsletter, January 15, 2005.
36. Хофман Б. Терроризм взгляд изнутри = Inside terrorism [пер. с англ.]. – М.: Ультра-культура, 2003.
37. Почепцов Г.Г. Информационные войны. – М.: Рефл-бук, К., Ваклер, 2000.
38. Панарин И. Технология информационной войны. Издательство «КСП+», 2003.
39. Benton D., Grindstaff F. Practical Guide to Computer Forensics: For Accountants, Forensic Examiners and Legal Professionals. «BookSurge Publishing», 2006.
40. Соловьев Л.Н. Классификация способов совершения преступлений, связанных с использованием и распространением вредоносных программ для ЭВМ.

41. Крылов В.В. Расследование преступлений в сфере информации. – М.: Городец, 1998.
42. Экспертизы на предварительном следствии: Краткий справочник / Под общ. ред. В.В.Мозякова. – М.: ГУ ЭКЦ МВД России, 2002.
43. Иванов Н.А. Применение специальных познаний при проверке «цифрового алиби» // журнал «Информационное право», 2006. №4 (7).
45. RFC-3954 «Cisco Systems NetFlow Services Export Version 9», 2004.
46. RFC-3917 «Requirements for IP Flow Information Export (IPFIX)», 2004.
47. Mikkilineni A.K., Chiang P.-J., Ali G.N., Chiu G.T.-C., Allebach J.P., Delp E.J. Printer Identification based on textural features / Proceedings of the IS&T's NIP20: International Conference on Digital Printing Technologies, Volume 20, Salt Lake City, UT, October/November 2004, pp. 306-311.
48. Горбатов В.С., Полянская О.Ю. Мировая практика криминализации компьютерных правонарушений. – М.: МИФИ, 1996.
49. Strombergson J., Walleij L., Faltstrom P. RFC-4194 «The S Hexdump Format», 2005.
50. Albert J. Marcella Jr., Robert S. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. «Greenfield», 2002.
51. Jansen W, Ayers R. Guidelines on PDA Forensics: Recommendations of the National Institute of Standards and Technology (NIST), Publ. SP-800-72, 2004.
52. Oseles L. Computer Forensics: The Key to Solving the Crime, 2001.
53. Feather C. RFC-3977 «Network News Transfer Protocol (NNTP)», 2006.
54. Adams R., Horton M. RFC-1036 «Standard for Interchange of USENET Messages», 1987.
55. Lonvick C. RFC-3164 «The BSD syslog Protocol», 2001.
56. Casey E. Practical Approaches to Recovering Encrypted Digital Evidence, 2002.
57. Jones K.J., Bejtlich R., Rose C.W. Real Digital Forensics: Computer Security and Incident Response. «Addison-Wesley Professional», 2005.
58. Bartle R.A. Pitfalls of virtual property, 2004 (http://www.themis-group.com/uploads/Pitfalls%20of%20Virtual%20Property.pdf).
59. Bisker S., Butterfield J., Jansen W., Kent K., Tracy M. Guidelines on Electronic Mail Security (Draft). Recommendations of the National Institute of Standards and Technology // NIST Publ. 800-45A.
60. Ayers R, Jansen W., Cilleros N., Daniellou R. Cell Phone Forensic

Tools: An Overview and Analysis / National Institute of Standards and Technology, NISTIR 7250, 2005.
61. Hare R.D., Hart S.D., Harpur T.J. Psychopathy and the DSM-IV Criteria for Antisocial Personality Disorder.
62. Moriarty L. Controversies in Victimology. «Anderson Publishing», Cincinatti, 2003.
63. Doerner W., Lab S. Victimology (4th edition). – «LexisNexis Anderson», Cincinnati, 2005.
64. Mohay G., Anderson A., Collie B., de Vel O., McKemmish R. Computer and Intrusion Forensics. – «Artech House», Boston, London, 2003.
65. Srijith K.N. Analysis of Defacement of Indian Web Sites // First Monday, volume 7, number 12 (December 2002).
66. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006.
67. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002.
68. Торвальд Ю. Сто лет криминалистики. – М.: Прогресс, 1974.
70. Середа С.А., Федотов Н.Н. Ответственность за распространение вредоносных программ для ЭВМ // Право и экономика. 2007, №3. С. 50-55.
71. Programming PHP. «O'Reilly», 2006.
72. Scambray J. Web Applications (Hacking Exposed). «McGraw-Hill», 2002.
73. Phishing Exposed. «Syngress Publishing», 2005.
74. Luna J.J. How to Be Invisible: The Essential Guide to Protecting Your Personal Privacy, Your Assets, and Your Life. «Thomas Dunne Books», 2004.
75. Anzaldua R., Volonino L., Godwin J. Computer Forensics: Principles and Practices. «Prentice Hall», 2006.
76. Шапиро И. Введение в типологию либерализма // журнал «Полис». 1994, №3. С. 7-12.
77. Быков П. Перспективы либерального консерватизма в России // журнал «Эксперт». 2007, №13.
78. Baker F., Foster B., Sharp C. RFC-3924: Cisco Architecture for Lawful Intercept in IP Networks. 2004.
79. Horrigan J.B. Home Broadband Adoption 2006. Pew Internet & American Life Project, 2006, 80.
80. Postel J. RFC-792: Internet Control Message Protocol. 1981, 81.
81. Середа С.А., Федотов Н.Н. Сложности толкования терминов «вредоносная программа» и «неправомерный доступ» // журнал «Российская юстиция». 2007, №2. С. 58-62.
82. Hoglund G., McGraw G. Exploiting Software: How to Break Code. «Addison Wesley», 2004.

83. Hoglund G., Butler J. Rootkits: Subverting the Windows Kernel. «Addison Wesley», 2005.
84. Ayers R., Jansen W. An Overview and Analysis of PDA Forensic Tools, Digital Investigation // The International Journal of Digital Forensics and Incident Response, Volume 2, Issue 2, April 2005.
85. Губанов В.А., Салтевский М.В., Щербаковский М.Г. Осмотр компьютерных средств на месте происшествия: Методические рекомендации. – Харьков: Академия правовых наук Украины, НИИ изучения проблем преступности, 1999.
86. Михайлов И.Ю. Методические рекомендации: Носители цифровой информации (обнаружение, изъятие, назначение компьютерно-технической экспертизы). – Курган: ЭКЦ при УВД Курганской области, 2003.
87. Spivey M.D. Practical Hacking Techniques and Countermeasures. «AUERBACH», 2006.
88. Азимов Э.Л., Щукин А.И. Словарь методических терминов (теория и практика преподавания языков). – СПб.: Златоуст, 1999.
89. Prosise C., et all. Incident Response and Computer Forensics (Second Edition), 2001.
90. Middleton B. Cyber Crime Investigator's Field Guide (Second Edition). «Auerbach», 2004.
91. Steel C. Windows Forensics: The Field Guide for Corporate Computer Investigations. «Wiley», 2006.
92. Ayers R., Jansen W. Forensic Software Tools for Cell Phone Subscriber Identity Modules // Conference on Digital Forensics, Association of Digital Forensics, Security, and Law (ADFSL), April 2006.
93. Jansen W, Ayers R. PDA Forensic Tools: An Overview and Analysis. NISTIR 7100, 2004.
94. Компьютерное пиратство: методы и средства борьбы: Методическое пособие. 8-е изд. – М.: НП ППП, 2005.
95. Lo C. «ATM Cameras Found by Chance» // South China Morning Post, 9 January 2004, p. 1.
96. Shepardson D. «Police Accuse Man of ATM Scheme» // The Detroit News, 5 December 2003.
97. Taylor N. «Bank Customers Warned of Hi-Tech Thievery at ATMs» // South China Morning Post, 16 December 2003, p. 3.
98 Федотов Н.Н. Реликтовое право // Закон и право. №4, 2007, с. 18-20.

Интернет-публикации

W01. Cellular/Mobile Phone Forensics.
http://www.e-evidence.info/cellular.html

W02. Computer Forensic Software Tools Downloads.
http://www.forensic-computing.ltd.uk/tools.htm
W03. Khalid. Introduction to Digital Archeology.
http://baheyeldin.com/technology/digital-archeology.html
W04. Пятиизбянцев Н. Проблемы уголовно-правовой борьбы с преступлениями в области банковских карт.
http://bankir.ru/analytics/Ur/36/66441
W05. Безмалый В.Ф. Мошенничество в Интернете // «Security Lab», 6 декабря 2006.
http://www.securitylab.ru/contest/280761.php
W06. Reverse IP DNS Domain Check Tool.
http://www.seologs.com/ip-domains.html
W07. Фальшивый сайт прокуратуры сделал Rambler? (обзор публикаций прессы). Компромат.Ru.
http://compromat.ru/main/internet/gprf1.htm
W08. В Интернете появился поддельный сайт Генпрокуратуры РФ // NewsRU. Новости России, 1 октября 2003.
http://www.newsru.com/russia/01oct2003/genprocuratura.html
W09. Поддельный сайт Генпрокуратуры предвосхищает действия настоящей Генпрокуратуры // NewsRU. Новости России, 3 октября 2003.
http://www.newsru.com/russia/03oct2003/site.html)
W10. Википедия. Список файловых систем.
http://ru.wikipedia.org/wiki/Список_файловых_систем
W11. Википедия. Сравнение файловых систем.
http://ru.wikipedia.org/wiki/Сравнение_файловых_систем
W12. Test Results for Disk Imaging Tools: dd Provided with FreeBSD 4.4 / National Institute of Justice, U.S. Department of Justice, 2004. Этот и другие отчёты NJI о тестировании доступны в Интернете:
http://www.ojp.usdoj.gov/nij/pubs-sum/203095.htm
http://www.ojp.usdoj.gov/nij/pubs-sum/200031.htm
http://www.ojp.usdoj.gov/nij/pubs-sum/200032.htm
http://www.ojp.usdoj.gov/nij/pubs-sum/199000.html
http://www.ojp.usdoj.gov/nij/pubs-sum/196352.htm
W13. Википедия. Информационная война.
http://ru.wikipedia.org/wiki/ Информационная_война
W14. США получили секретные коды для слежки за гражданами мира через принтеры.
http://vkabinet.ru/articles.php?aid=1
http://www.newsru.com/world/20oct2005/printer.html#1
W15. DocuColor Tracking Dot Decoding Guide.
http://www.eff.org/Privacy/printers/docucolor/

W16. Is Your Printer Spying On You?
http://www.eff.org/Privacy/printers/
W17. Purdue Sensor and Printer Forensics (PSAPF).
http://cobweb.ecn.purdue.edu/~prints/
W18. Википедия: Hex dump.
http://en.wikipedia.org/wiki/Hexdump
W19. Спецификация алгоритма «yEnc».
http://www.yenc.org/
W20. Перечень и сравнительные характеристики клиентов файлообменных сетей.
http://en.wikipedia.org/wiki/Comparison_of_file_sharing_applications
W21. P2P-сервисы выходят на следующий этап своего развития // «Security Lab», 3 ноября 2006
http://www.securitylab.ru/news/276373.php
W22. Тутубалин А. RBL: вред или польза? // Электронный журнал «Спамтест»
http://www.spamtest.ru/document.html?pubid=22&context=9562
W23. Федотов Н.Н. О «черных списках» фильтрации почты // Электронный журнал «Спамтест».
http://www.spamtest.ru/document.html?pubid=8&context=9562
W24. Собецкий И.В. О доказательственном значении лог-файлов // «Security Lab», 25 июля 2003.
http://www.securitylab.ru/analytics/216291.php
W25. Sarangworld Traceroute Project Known Hostname Codes.
http://www.sarangworld.com/TRACEROUTE/showdb-2.php3
W26. Fingerprint Sharing Alliance.
http://www.arbornetworks.com/fingerprint-sharing-alliance.php
W27. Antisocial Personality Disorder for professionals. Armenian Medical Network.
http://www.health.am/psy/more/antisocial_personality_disorder_pro/
W28. Forensic Examination of Computers and Digital and Electronic Media (IACIS).
http://www.iacis.info/iacisv2/pages/forensicprocprint.php
W29. Собецкий И.В. Организация технико-криминалистической экспертизы компьютерных систем // «Security Lab», 10 ноября 2003.
http://www.securitylab.ru/analytics/216313.php

Нормативные акты

L01. Постановление Правительства РФ от 27 августа 2005 г. №538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность» // Собрание законодательства Российской Федерации, №36, 05.09.2005, ст. 3704.
L02. Постановление Пленума Верховного Суда Российской Федерации №15 от 19 июня 2006 г. «О вопросах, возникших у судов при рассмотрении гражданских дел, связанных с применением законодательства об авторском праве и смежных правах».
L03. Правила регистрации доменных имен в домене RU – нормативный документ Координационного центра национального домена сети Интернет, утвержден решением П2-2.1, 4.1/06 от 24.04.2006.
L04. Федеральный закон «Об оценочной деятельности в Российской Федерации» от 29 июля 1998 г. (№135-ФЗ).
L05. Закон РФ «О коммерческой тайне» (№98-ФЗ).

Официоз или сленг?

Словарь официальных и жаргонных технических терминов

Терминология в области ИТ пока неустоявшаяся. К тому же отрасль стремительно развивается, и новые термины появляются, распространяются и забываются достаточно быстро. Зачастую появляются они сразу в нескольких вариантах.

Автору неоднократно приходилось наблюдать специалиста, застывшего в затруднении над официальным или полуофициальным документом, – как правильно написать, какой термин употребить, чтобы было понятно и чтобы не скатиться до технического сленга, на котором в основном и общаются компьютерщики? Еще более строгие требования в отношении терминологии предъявляются к процессуальным документам. Здесь ошибка в терминологии может привести к отказу в рассмотрении доказательства («документ составлен не на русском языке»), а то и к судебной ошибке.

Ниже приводятся проблемные термины из области ИТ, как официальные, так и жаргонные.

Жирным шрифтом выделены официальные термины, закрепленные в тех или иных нормативных актах (см. сноски) или просто часто применяемые в официальных документах, и потому приемлемые.

Курсивом выделены жаргонные термины, техницизмы, новая и неустоявшаяся терминология, которую использовать в процессуальных документах не рекомендуется.

Обычным шрифтом набраны термины, занимающие промежуточное положение. Их вполне можно употреблять в официальных документах, но при этом рекомендуется тем или иным образом пояснять их, дабы не возникло путаницы.

Критерием официальности термина для данного словаря считается употребление этого термина в российских законах, подзаконных нормативных актах, иных официальных документах. Если такое употребление отсутствует, то выбран тот термин, который используется большинством специалистов.

cc – **кредитная карта**; обобщенно – любая **банковская карта**

CD – см. **компакт-диск**

CD-R – записываемый **компакт-диск**, разновидность диска с возможностью однократной записи

CD-ROM – (1) **компакт-диск**, разновидность без возможности записи; (2) устройство (привод) для чтения компакт-дисков

CD-RW – записываемый **компакт-диск**, разновидность с возможностью многократной записи

CPU – см. **процессор**

chargeback – см. **возврат платежа**

cheating – см. читинг

DNS[1], *ДНС*, служба доменных имён – система доменных имен, а также система серверов, осуществляющих разрешение доменных имен (DNS-серверов)

DoS-атака – **атака типа «отказ в обслуживании»** на компьютерную сеть, отдельный компьютер или информационную систему

DRM (digital rights management) – см. **техническое средство защиты авторских прав**

hub – см. **концентратор**

ICQ[2] **(ай-си-кью)**, *аська* – программа и протокол, предназначенные для мгновенного обмена текстовыми сообщениями между пользователями персональных компьютеров через сеть

ISP (internet service provider) – см. интернет-провайдер

IP-адрес[3], IP, айпи, *айпишник* – сетевой адрес узла для протокола IP

floppy-disk, floppy-диск – см. **дискета**

malware – см. **вредоносная программа**

merchant, мерчант – предприятие, соглашающееся принимать платежи по банковским картам; действует по договору с банком-эквайром

merchant account, *мерчант-аккаунт* – специальный открываемый продавцом транзитный счет в **банке-эквайре**, который позволяет принимать платежи по банковским картам; открывая такой счет, банк соглашается платить продавцу за правильно совершенные покупки в обмен на снятие денег со счетов покупателей в **банках-эмитентах**

MX (mail exchange), *эм-икс, эм-экс* – (1) сервер входящей электронной почты, соответствующий домену электронной почты; (2) тип DNS-записи, указывающей на сервер входящей электронной почты для домена (также: MX-запись)

newsgroups – см. **телеконференции**

---

[1] Термин использован в двух приказах Мининформсвязи (от 10.01.2007 №1 и от 24.08.2006 №113), в нескольких нормативных актах субъектов Федерации, а также в ряде судебных решений.

[2] Термин не упоминается в федеральных законах, но упоминается в двух постановлениях правительства Москвы (№656 ПП от 30.08.2005 и №646 ПП от 29.08.2006), распоряжениях других органов власти субъектов Федерации, ряде подзаконных актов.

[3] Термин упоминается в двух приказах Минсвязи (№166 от 11.12.2006 и №112 от 24.08.2006), двух указаниях ЦБ (№1390-У от 01.03.2004 и №1376-У от 24.11.2006), нескольких десятках постановлений и распоряжений органов власти субъектов федерации.

NIC – см. **сетевая карта**
patch – см. **обновление**
RAM – см. **ОЗУ**
rootkit – см. руткит
RTFM – read the following manual (*read the fucking manual*), фраза используется в качестве указания или совета прочесть инструкцию, а не задавать никчемных вопросов
screensaver – см. скринсейвер
screenshot – см. скриншот
script kiddie, скрипт-кидди, script bunny, script kitty, script kiddo, «skidiot» – компьютерный злоумышленник, который из-за недостатка знаний совершает сетевые атаки при помощи готовых программ, написанных другими людьми, обычно пользуется ими, не понимая того, как они устроены и работают
SIM-карта, *симка* – карта, с помощью которой обеспечивается идентификация абонентской станции (абонентского устройства), ее доступ к сети подвижной связи, а также защита от несанкционированного использования абонентского номера[4]
skimming – см. скиминг
SMS – см. **короткое текстовое сообщение**
sniffer – см. снифер
socks-сервер – сервер, предоставляющий услуги по пробросу соединений по протоколу SOCKS (RFC 1928); используется в целях анонимизации доступа; по своему принципу действия похож на прокси-сервер, но не ограничивается протоколом HTTP и имеет более широкие возможности
swap, swap-файл – см. **файл подкачки**
upgrade – см. **модернизация**
UPS – см. **источник бесперебойного питания**
Usenet – см. **телеконференции**
warez – см. *варез*
web-сайт – см. **веб-сайт**
адрес электронной почты, адрес, мейл-адрес, e-mail address, *е-мейл* – символьное обозначение, идентифицирующее место доставки сообщения **электронной почты**, почтовый ящик
айти, ай-ти – см. **ИТ**
акка́унт (account) – см. **учетная запись пользователя**
апгре́йд – см. **модернизация**
аппаратная часть, hardware, *хард, хардвер, железо* – обобщающее название для материальной составляющей компьютерной техники; термин применяется в основном при сопоставлении программной и аппаратной части (*софт* и *хард*)

[4] Термин и определение содержатся в Правилах оказания услуг подвижной связи – см. постановление Правительства РФ «Об утверждении правил оказания услуг подвижной связи» от 25 мая 2005 г. №328.

аська – см. **ICQ**
аутентификация[5] (authentication) – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности; в качестве указанного идентификатора чаще всего выступают **логин** и пароль
банковская (платежная) карта[6], карта, карточка – средство для составления расчетных и иных документов, подлежащих оплате за счет клиента; пластиковая карточка стандартных размеров 85,6 x 53,9 x 0,76 мм с магнитной полосой или микросхемой; идентификация держателя обеспечивается нанесением на карту номера, срока действия, фамилии, имени и образца подписи держателя карты
баннер, рекламный баннер[7] – изображение стандартизованного размера (468*60, 100*100 или др.), несущее рекламную информацию, предназначенное для размещения на веб-странице; реже баннер бывает текстовым или flash-объектом; часто баннер размещается не непосредственно веб-мастером, а через систему обмена баннерами (баннерообменную систему)
белый IP-адрес – см. публичный IP-адрес
бесперебойный источник питания – см. **источник бесперебойного питания**
билинговая система – см. **автоматизированная система расчетов**
ботнет – см. зомби-сеть
брандмауэр – см. **межсетевой экран**
бра́узер[8] (browser), **веб-браузер**[9], интернет-браузер[10], бро́узер, обозреватель, веб-клиент – программа для просмотра **веб-страниц** и иных сетевых информационных ресурсов; установлена на персональном компьютере пользователя, взаимодействует по сети с **веб-сервером**, запрашивает и принимает от него данные (обычно на языке HTML), обрабатывает и показывает их в виде веб-страницы; браузер является типичной **клиентской частью**, которой соответствует **веб-сервер**

[5] Термин определен в руководящем документе Гостехкомиссии «Защита от несанкционированного доступа к информации. Термины и определения».
[6] Термин определен в «Положении об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт» от 24 декабря 2004 г. №266-П (в ред. Указания ЦБ РФ от 21.09.2006 № 1725-У).
[7] Термин используется в письме Федеральной антимонопольной службы от 17 сентября 2004 г. №АК/5841 «О применении пункта 1.1 статьи 16 Федерального закона «О рекламе», а также в ряде ведомственных актов и судебных решений.
[8] Термин встречается в нескольких десятках ведомственных нормативных актов, иногда с префиксами «веб-» или «интернет-».
[9] См., например, распоряжение Правительства РФ от 24 апреля 2007 г. №516-р.
[10] В такой форме термин встречается в трех указаниях Центрального банка РФ.

как **серверная часть**

бэк-офис (back office) – часть **информационной системы** или интерфейса информационной системы, ориентированная на собственных сотрудников предприятия; термин используется при сопоставлении с фронт-офисом

варез, wares, warez – пользующееся популярностью программное обеспечение, обычно контрафактное; термин применяется в основном к контенту сайтов

веб[11], web – первая часть (префикс) сложных слов, означающая их отношение к системе гипертекстовых страниц (WWW); пишется через дефис

веб-мейл – см. **веб-интерфейс сервера электронной почты**

веб-интерфейс сервера электронной почты, *веб-мейл* – клиент электронной почты, сделанный в виде программы, работающей на сервере и взаимодействующей с пользователем по протоколу http через браузер

веб-мастер – человек, осуществляющий изготовление и/или обслуживание **веб-сайтов**

веб-обозреватель[12] – см. **браузер**

веб-порта́л, портал – большой и сложный по структуре **веб-сайт**, либо объединение взаимодействующих между собой веб-сайтов

веб-сайт[13], web-сайт, **сайт**[14], интернет-сайт[15] – информационный ресурс, доступный пользователю по протоколу HTTP или HTTPS; с точки зрения пользователя, представляет собой совокупность **веб-страниц**; с точки зрения администратора и изготовителя (веб-мастера), представляет собой совокупность данных на языке HTML, графических изображений, программ и других данных, а также веб-сервера, который на основе этих данных формирует ответы пользователям; с точки зрения авторского права может рассматриваться как сложный объект, включающий программы для ЭВМ, базы данных, текст, графические произведения и др.

[11] Части (префиксы) «web-» и «веб-» употребляются в нормативных актах примерно с равной частотой. Например, в постановлениях и решениях Правительства РФ: «веб» – 15, «web» – 4; в указах Президента РФ: «веб» – 1, «web» – 1; в актах правительства Москвы: «веб» – 25, «web» – 55. Рекомендуется использовать префикс «веб-», чтобы избежать придирок, что, дескать, «документ составлен не на русском языке».

[12] В таком варианте термин содержится в единственном нормативном документе – Постановлении Правительства РФ от 10 марта 2007 г. №147 «Об утверждении положения о пользовании официальными сайтами...». В прочих нормативных документах использован термин «браузер» или «броузер».

[13] Термин употребляется в нескольких ведомственных приказах, а также в нескольких судебных решениях, например, в распоряжении Правительства РФ от 1 июля 2006 г. №944-р или в письме Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека от 4 декабря 2006 г. №0100/12859-06-32 «О проведении Всероссийского форума «Здоровье нации – основа процветания России».

[14] Хотя термин «сайт» встречается в нормативных актах чаще, чем термин «веб-сайт», автор все же рекомендует для официального употребления «веб-сайт». Дело в том, что «сайт» – более широкое понятие, чем «веб-сайт». Слово «сайт» используется в нормативных актах тогда, когда из контекста понятно, что речь идет именно о «веб-», а не о каком-либо другом сайте.

[15] Термин часто используется в решениях судов.

веб-сервер – программа, установленная на сервере и осуществляющая взаимодействие браузера пользователя с **веб-сайтом** по протоколу HTTP или HTTPS

веб-страница – результат представления в браузере информации (обычно на языке HTML), передаваемой пользователю **веб-сервером**; элемент веб-сайта

взлом – см. несанкционированный доступ

винчестер – см. **НЖМД**

вирмейкер – изготовитель **вредоносных программ**, вирусописатель

вирь – см. **вредоносная программа**

вирус, **компьютерный вирус**, *вирь* – (1) программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия, при этом копии сохраняют способность дальнейшего распространения; относится к вредоносным программам[16]; (2) вредоносная программа вообще

возврат платежа, chargeback, *чарджбэк* – возврат платежа, совершенного по банковской карте; сумма, которую вычитают со счета продавца по требованию держателя карты; инициируется эмитентом по заявлению держателя, после того как эквайер завершил транзакцию; по каждому случаю проводится разбирательство, если признана правота держателя карты, у продавца со счета вычитают сумму платежа плюс плату за возврат (chargeback fee)

вредоносная программа, вирус, malware – программа для ЭВМ, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети[17]; типы вредоносных программ: вирус, червь, троянская программа, логическая бомба, эксплоит, руткит, комбинированная

гибкий магнитный диск (ГМД) – см. **дискета**

группы новостей – см. **телеконференции**

дамп банковской (платежной) карты – копия содержимого магнитной полосы карты; снимается обычно с целью изготовления твердой копии такой карты

дамп памяти – см. **содержимое ОЗУ**

[16] Определение из ГОСТ Р 51188-98.

[17] Термин определен в УК РФ, ст. 273.

декомпилирование программы для ЭВМ, декомпиляция – технический прием, включающий преобразование **объектного кода** в **исходный текст** в целях изучения структуры и кодирования программы для ЭВМ[18]

дефейс, дифейс, deface – изменение (частичное или полное) страницы чужого веб-сайта (обычно титульной) для демонстрации результативного несанкционированного доступа; применяется для удовлетворения тщеславия, публичной демонстрации уязвимости или для дискредитации владельца сайта

директория, каталог, *папка* – файл особого типа, содержащий в себе заголовки других файлов (в том числе и других директорий); присуща подавляющему большинству файловых систем

дискета[19], гибкий диск, гибкий магнитный диск[20] (ГМД), флоппи-диск, *флоп* – носитель компьютерной информации

дистрибутив[21], инсталляционный пакет – пакет, набор данных, предназначенный для инсталляции (установки) программы для ЭВМ; как правило, включает в себя архив с программой и программу-инсталлятор (установщик), либо инструкции для программы-инсталлятора или для пользователя

доме́н[22] – область (ветвь) иерархического пространства доменных имен сети Интернет, которая обозначается уникальным **доменным именем**

доме́нное имя[23] – уникальный символьный идентификатор домена; служит для адресации узлов сети Интернет и расположенных на них сетевых ресурсов в удобной для человека форме; для обеспечения уникальности и защиты прав владельцев доменные имена 1-го и 2-го (в отдельных случаях и 3-го) уровней можно использовать только после их регистрации, которая производится уполномоченными на то регистраторами

[18] Термин определен в законе РФ «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992 №3523-I), ч. 1 ст. 1.

[19] Термин не встречается в законах, но многократно упоминается в нормативных документах ЦБ РФ и Минфина РФ, например, в письме Московского ГТУ ЦБР от 5 декабря 2006 г. №30-01-01/82512 «О программе подготовки отчетности по форме 0409664» или в письме Департамента налоговой и таможенно-тарифной политики Минфина РФ от 12 июля 2006 г. №03-02-07/1-178.

[20] Термин не встречается в законах. Эпизодически упоминается (всего около 10 случаев) в ведомственных приказах, например, в приказе Федеральной службы по экологическому, технологическому и атомному надзору от 6 октября 2006 г. №873 «Об утверждении и введении в действие Типовой инструкции о защите информации в автоматизированных средствах центрального аппарата, территориальных органов и организаций Федеральной службы по экологическому, технологическому и атомному надзору».

[21] Термин используется в нормативных документах ЦБ РФ, например, письмо Московского ГТУ ЦБР от 19 января 2007 г. №30-01-01/3486 «О консолидированной отчетности».

[22] Термин определен в документе «Правила регистрации доменных имен в домене RU», утвержден решением Координационного центра национального домена сети Интернет №П2-2.1,4.1/06 от 24.04.2006 (http://cctld.ru/ru/doc/acting/?id21=13&i21=1).

[23] Термин упоминается в законе «О товарных знаках...», ч. 2 ст. 4, а также в ч. 4 ГК РФ.

доме́н электронной почты – совокупность адресов электронной почты, относящихся к одному доменному имени и, как следствие, имеющих общий сервер входящей электронной почты (**MX**)

донкей, е-донкей, осел, мул, е-мул – клиентские программы **файлообменных сетей**

думатель – см. **процессор**

доступ к информации – возможность получения информации и ее использования[24]

е-мейл – (1) см. **электронная почта**; (2) см. **адрес электронной почты**

железо – см. **аппаратная часть**

заставка – см. скринсейвер

захват доменов – см. **киберсквоттинг**

зомби-сеть, *ботне́т* (botnet) – группа компьютеров, зараженных вредоносной программой типа «троянский конь», управляемых из единого центра; как правило, такая сеть структурированная, с резервными управляющими связями; используется для рассылки спама, организации атак, сокрытия истинных источников трафика и других задач; может насчитывать от единиц до десятков тысяч компьютеров

ине́т – см. **Интернет**

инсталляционный пакет – см. **дистрибутив**

инсталляция[25], инсталляция программного обеспечения, установка[26] программного обеспечения – процесс развертывания **программного обеспечения** на **НЖМД** компьютера, где оно будет непосредственно запускаться; чаще всего происходит из **дистрибутива** путем запуска специализированной программы-инсталлятора (установщика)

Интернет[27], **сеть «Интернет»**, **международная компьютерная сеть Интернет**, глобальная компьютерная сеть, *инет*, *тырнет*, Сеть – глобальная компьютерная сеть, объединение компьютерных сетей; имеет два аспекта: технический и социальный; с технической точки зрения представляет собой совокупность узлов, соединенных линиями

[24] Термин и определение содержатся в ФЗ «Об информации, информационных технологиях и о защите информации» (№149-ФЗ), ст. 2.

[25] Термин использован в некоторых ведомственных актах, например, в приказе Министерства информационных технологий и связи РФ от 3 октября 2006 г. №128 и в письме Министерства образования и науки РФ от 26 мая 2006 г. №01-295/08-01.

[26] Термин изредка используется в судебных решениях. Автор затрудняется сделать выбор между терминами «инсталляция» и «установка программного обеспечения» и рекомендует в официальных документах использовать оба термина: «инсталляция (установка) программного обеспечения».

[27] Термин содержится в 46 федеральных законах РФ – везде по-русски и с прописной буквы.

связи, работающих по единым протоколам; с социальной точки зрения представляет собой среду для обмена информацией между лицами, почти не зависящую от географического расположения, государственных границ, социального положения

интернет-казино, онлайновое казино, онлайн-казино – заведение игорного бизнеса, либо виртуальное, то есть целиком размещенное в Сети, либо реальное, но имеющее сетевой интерфейс для принятия ставок и получения выигрышей

интернет-провайдер, провайдер, ISP – **оператор связи**, имеющий лицензию на такие услуги связи, как передача данных, услуги телематических служб, аренда каналов связи

интернет-сайт – см. **веб-сайт**

информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[28]; **информационной системой** часто можно с полным основанием назвать «ЭВМ, систему ЭВМ, их сеть», как этот объект именуется в ст. 273 УК

информационное содержание, конте́нт – наполнение веб-сайта или иного сетевого информационного ресурса: текст, изображения, музыка, видео и т.п.

источник бесперебойного питания[29] (ИБП), бесперебойный источник питания, UPS, *УПС* – устройство, подключаемое между компьютером и электрической сетью, позволяющее некоторое время поддерживать электропитание при отключении или падении внешнего

исполняемый код – см. **объектный код**

исходный текст программы[30], *исходник*, исходный код, source-code, *сорс-код*, *сорцы*, *сырцы* – исходный текст программы для ЭВМ на **алгоритмическом языке** высокого уровня; он не исполняется компьютером непосредственно, но преобразуется компилятором в исполняемый код (**объектный код**)

ИТ (информационные технологии), IT, ай-ти – отрасль знаний и отрасль экономики, связанная с компьютерами, программами для ЭВМ, компьютерными сетями; тесно связана с отраслью связи, но не включает ее

камень – см. **процессор**

[28] Термин и определение содержатся в ФЗ «Об информации, информационных технологиях и о защите информации» (№149-ФЗ), ст. 2.

[29] Термин встречается в трех постановлениях Правительства РФ (например, от 29 марта 2007 г. №190 «О НОРМАХ ОБЕСПЕЧЕНИЯ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ...»), в 29 ведомственных приказах, многочисленных нормативных актах субъектов Федерации.

[30] Термин использован в законе РФ «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992 №3523-I), ч. 3 ст. 3.

ка́рдер – преступник, занимающийся мошенничеством с банковскими (платежными) картами, а именно неправомерным получением данных таких карт, их применением для приобретения товаров и услуг, изготовлением копий таких карт, их использованием в магазинах и банкоматах

кардинг – мошенничество с банковскими (платежными) картами

каталог – см. **директория**

киберскво́ттер – лицо, зарабатывающее торговлей доменными именами

киберсквоттинг, cybersquotting, *сквоттинг*, захват доменов – приобретение доменных имен с целью их последующей перепродажи или недобросовестного использования

клиент – см. **клиентская часть программы**

клиентская часть программы – та часть или модуль программы или комплекса программ, построенной по архитектуре «клиент-сервер», которая инициирует вызовы

клиент электронной почты, почтовая программа, почтовый клиент, MUA, *мейлер* – программа, имеющая функции создания, отправки, приема, показа и хранения сообщений электронной почты; работает на персональном компьютере пользователя. Популярные клиенты: «Eudora Mail», «Mozilla Thunderbird», «Netscape Mail», «Outlook», «Outlook Express», «The Bat!»

колока́ция (collocation, co-location), *колокейшн* – услуга оператора связи, состоящая в размещении сервера клиента на узле связи (датацентре) оператора и подключении его к высокоскоростной линии связи; обычно держать свой сервер на чужом узле связи выгоднее, чем тянуть линию связи до собственного офиса

коммутатор[31], *свич* (switch) – сетевое коммуникационное устройство, осуществляющее коммутацию фреймов, работает на 2-м уровне, используется для соединения компьютеров в рамках одного сегмента компьютерной сети

компакт-диск[32], CD, *компакт* – носитель компьютерной информации

компьютер[33], **ЭВМ**[34], *комп*, машина, *тачка*, рабочая станция, персональный компьютер, ПК, *писюк* – универсальное техническое средство для обработки информации

контент – см. **информационное содержание**

контрафактный экземпляр, нелицензионная копия, *пиратский экземпляр*

[31] Термин упоминается в приказе Минсвязи №158 от 07.12.2006 и др. нормативных актах.

[32] Термин объяснен в «Словаре методических терминов» [88].

[33] Термин содержится в 23 федеральных законах РФ, например, в ст. 346.25.1 НК, ст. 259 УПК РФ.

[34] Термин используется в законе «О правовой охране программ для ЭВМ и баз данных»; всего термин содержится в 56 федеральных законах РФ.

– экземпляр произведения (программы, фонограммы), изготовление или распространение которого влечет за собой нарушение авторских и смежных прав[35]

концентратор[36], сетевой концентратор, hub, *хаб* – сетевое коммуникационное устройство, осуществляющее распространение (повторение) фреймов, работает на 2-м уровне, используется для соединения компьютеров в рамках одного сегмента компьютерной сети; в отличие от коммутатора, каждый полученный фрейм посылает не в один, а во все порты; как правило, не конфигурируется и не управляется

короткое текстовое сообщение, SMS, СМС, *эсэмэс*, *эсэмэска* – сообщение, состоящее из букв или символов, набранных в определенной последовательности, предназначенное для передачи по сети подвижной связи[37]

кракер – человек, осуществляющий модификацию (как правило, недозволенную) компьютерных программ; создатель *кряков*

креда – см. **банковская карта** или **кредитная карта**

кредитная карта[38] – вид **банковской карты**

криптодиск, криптоконтейнер – (1) программа, создающая и поддерживающая работу виртуального диска, вся информация на котором зашифрована, при записи и считывании она шифруется и расшифровывается «на лету», прозрачно для пользователя; (2) сам этот виртуальный диск

кряк, крак, crack – программа или инструкция для обхода, отключения, иного преодоления **технических средств защиты авторских прав**

ла́мер – малоквалифицированный пользователь ЭВМ, обычно еще и считающий себя квалифицированным, то есть воинствующий *чайник*; распространенная среди технических специалистов негативная характеристика, ругательство, оскорбление

лог, лог-файл – компьютерный журнал регистрации событий; файл или база данных с записями о событиях, относящихся к определенной информационной системе или программе

логин[39] (login), учетное имя пользователя – символьный идентификатор

[35] Определение термина взято из ч. 3 ст. 48 закона «Об авторском праве и смежных правах» (в ред. Федеральных законов от 19.07.1995 №110-ФЗ, от 20.07.2004 №72-ФЗ).

[36] Термин упоминается в приказе Минсвязи №158 от 07.12.2006 и др. нормативных актах.[37] Термин и определение содержатся в Правилах оказания услуг подвижной связи – см. постановление Правительства РФ «Об утверждении правил оказания услуг подвижной связи» от 25 мая 2005 г. №328.

[38] Термин определен в «Положении об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт» от 24 декабря 2004 г. №266-П (в ред. Указания ЦБ РФ от 21.09.2006 №1725-У).

[39] Термин замечен в официальных документах единожды – см. письмо Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека от 19 апреля 2006 г. №0100/4492-06-32 «О системе автоматизированного учета выдачи личных медицинских книжек и санитарных паспортов».

учетной записи пользователя; часто используется вместе с паролем для **аутентификации**

логическая бомба – вид программы (иногда признается вредоносной), цель которой уничтожить на компьютере, где она установлена, наиболее чувствительные данные; срабатывает при выполнении или при невыполнении заранее определенных условий, например, в заданное время

локальная сеть, **локальная вычислительная сеть, ЛВС**, *локалка*, LAN – компьютерная сеть местного уровня (офис, дом, подъезд); состоит обычно из одного сегмента

мануа́л (manual), *ман* – инструкция, **руководство пользователя**, справочное руководство к программе или компьютерной технике

маршрутиза́тор[40], роутер (router), *рутер* – сетевое коммуникационное устройство, осуществляющее маршрутизацию пакетов (чаще всего по протоколу IP), работает на 3-м уровне, используется для соединения различных сегментов компьютерной сети

межсетевой экран[41], сетевой экран, firewall, *файервол*, брандмауэр – устройство для защиты от сетевых атак, работающее в основном на 3-м уровне

мерчант – см. merchant

модернизация, *апгрейд* (upgrade) – замена комплектующих в компьютерной технике с целью улучшения ее характеристик; обычно этот термин применяется лишь к аппаратной части, а для программ используются другие термины

мыло – см. **электронная почта**

НЖМД (накопитель на жестком магнитном диске), **жесткий диск**, диск, винчестер, HD, *хард-драйв, хард* – устройство для долговременного энергонезависимого хранения компьютерной информации

несанкционированный доступ[42] (НСД) – доступ к информационной системе или к компьютерной информации в нарушение установленного порядка; этот термин является техническим, в отличие от юридического термина «неправомерный доступ», хотя означает почти то же самое

ньюсгруппы – см. **телеконференции**

ньюсридер – программный клиент для работы с **телеконференциями**

[40] Термин используется в Постановлении Правительства РФ от 18 ноября 2006 г. №697 «О внесении изменений в Классификацию основных средств, включаемых в амортизационные группы», а также в нескольких ведомственных актах.

[41] Термин определен в документе «Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Руководящий документ ГТК.

[42] Термин определен в руководящем документе Гостехкомиссии «Защита от несанкционированного доступа к информации. Термины и определения».

обновление[43], *патч* (patch) – программа или набор данных с инструкцией по установке, предназначенный для модернизации отдельной программы для ЭВМ или целой информационной системы с целью увеличения ее функциональности или исправления ошибок; не имеет самостоятельной ценности, используется только вместе с обновляемой программой; обычно обновления выпускает тот же производитель, который выпустил обновляемую программу, но иногда встречаются и обновления, выпущенные иными лицами

обозреватель – см. **браузер**

объектный код[44], исполняемый код – откомпилированный код программы для ЭВМ в машинных командах; не предназначен для восприятия человеком; получается из исходного текста методом компиляции

ОЗУ (оперативное запоминающее устройство), **оперативная память**, память, *мозги*, RAM – энергозависимое устройство для хранения компьютерной информации с быстрым произвольным доступом

онла́йн (on line), онлайновый – нечто, связанное с действиями в компьютерной сети, размещенное в сети, виртуальное; термин часто употребляется в сопоставлении с существующим в реальном мире, материальным

онлайн-казино – см. интернет-казино

оператор связи[45] – предприятие, имеющее лицензию на один или несколько видов услуг связи; предприятие, оказывающее услуги связи

операционная система[46] (ОС), система, *ось*, *операционка* – главная программа, управляющая работой всех других программ на компьютере

орган самоуправления Интернета – см. **саморегулируемая организация**

офла́йн (off line), офлайновый – нечто происходящее в реальном мире; применяется как противопоставление онлайновому

партиция (partition) – см. **раздел диска**

патч (patch) – см. **обновление**

патчер (patcher) – программа или часть программы, служащая для автоматизации скачивания и установки **обновлений** (*патчей*)

[43] Термин «обновление» в отношении программ для ЭВМ и БД используется в ст.ст. 263, 346.5 и 346.16 Налогового кодекса РФ, а также в нескольких указах Президента РФ, нескольких ведомственных актах. Термин «обновление» в отношении баз данных используется в ст. 1335 ГК РФ (вступает в силу 01.01.2008).44 Термин использован в Законе РФ «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992 №3523-I), ч. 3 ст. 3.

[45] Термин определен в законе «О связи».

[46] Не найдено упоминания этого термина в законодательстве. В ведомственных нормативных актах упоминается, но не часто. В то же время следует отметить, что альтернативных терминов просто не существует.

патч-корд[47] – короткий соединительный кабель для соединения разъемов коммутационной панели (патч-панели); также патч-кордом иногда не вполне корректно именуют соединительный кабель для подключения оконечного оборудования к коммутатору

пиратский – см. **контрафактный**

письмо – **сообщение электронной почты**

почтовый ящик – каталог или файл на сервере электронной почты, в который складываются полученные сообщения для какого-либо пользователя; обычно однозначно ассоциируется с **адресом электронной почты**

подкачка – см. **файл подкачки**

предмет письма – **поле «Subject» в сообщении электронной почты**

предоплаченная карта[48] – вид **банковской карты**

приватный IP-адрес, *серый IP-адрес* – IP-адрес, принадлежащий к одному из специальных диапазонов (см. RFC-1918), предназначенный для использования во внутренних компьютерных сетях, не имеющих непосредственной связи с Интернетом

приложение – см. **программа для ЭВМ**

провайдер – см. интернет-провайдер

программа для ЭВМ, программа, компьютерная программа, приложение, application, исполняемый код, скрипт – объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата[49]

программное обеспечение, ПО, software, *софт*, *софтвер* – обобщающее название для **программ для ЭВМ**; термин применяется в основном при сопоставлении программной и **аппаратной части** (*софт* и *хард*)

протокол коммуникационный, протокол, протокол обмена – свод правил обмена данными между различными программами, устройствами, информационными системами; обычно определяется техническим стандартом; соблюдение двумя программами единого протокола является необходимым условием их совместимости

проц – см. **процессор**

процессор, *проц*, *камень*, *думатель*, ЦПУ, **CPU** – центральный процессор компьютера или коммуникационного устройства; устройство, осу-

[47] Термин использован в приказе Министерства здравоохранения и социального развития РФ от 19 марта 2007 г. №178, распоряжении первого заместителя мэра Москвы в правительстве Москвы от 27 марта 2007 г. №53-РЗМ и некоторых других ведомственных документах.48 Термин определен в «Положении об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт» от 24 декабря 2004 г. №266-П (в ред. Указания ЦБ РФ от 21.09.2006 №1725-У).

[49] Определение термина взято из ст. 4 закона «Об авторском праве и смежных правах» (в ред. федеральных законов от 19.07.1995 №110-ФЗ, от 20.07.2004 №72-ФЗ).

ществляющее арифметическо-логические операции и управляющее работой всех остальных устройств компьютера

публичный IP-адрес, *белый IP-адрес* – IP-адрес, не являющийся приватным, маршрутизируемый всеми узлами Интернета; за исключением некоторых случаев, является уникальным идентификатором устройства в сети Интернет

раздел диска, раздел, partition, партиция – область диска, выделенная при разметке для размещения отдельной **файловой системы** (логического диска)

расчетная (дебетовая) карта[50] – вид **банковской карты**

релей, relay – промежуточный **сервер электронной почты**, принимающий сообщения для пользователей, почтовые ящики которых расположены не на нем, и пересылающий эти сообщения другому серверу

ро́утер – см. **маршрутизатор**

рутер – см. **маршрутизатор**

руткит (rootkit) – вид **вредоносной программы**, которая обычно применяется злоумышленником уже после получения доступа к чужому компьютеру, она предназначена для повышения привилегий, сокрытия «присутствия» злоумышленника на компьютере и его действий

сайт – (1) см. **веб-сайт**; (2) любой сетевой информационный ресурс

саморегулируемая организация[51], орган саморегулирования Интернета, орган самоуправления Интернета – организация, в силу соглашения, назначения или традиции исполняющая какие-либо функции по управлению работой Интернета, установлению правил работы, разработке технических стандартов; примеры таких организаций: IANA, IETF, регистраторы доменных имен, регистраторы IP-адресов

свич – см. **коммутатор**

своп, своп-файл – см. **файл подкачки**

свопинг (swapping) – (1) см. **файл подкачки**; (2) процесс обмена между реальной оперативной памятью и виртуальной, то есть областью подкачки

сервер – (1) компьютер, ориентированный на обслуживание многих пользователей или на управление работой компьютерной сети; (2) см. **серверная часть программы**

серверная часть программы – часть или модуль программы или комплекса

[50] Термин определен в «Положении об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт» от 24 декабря 2004 г. №266-П (в ред. Указания ЦБ РФ от 21.09.2006 №1725-У).

[51] Термин использован в ч. 2 ст. 15 ФЗ «Об информации...», там же установлен статус таких организаций.

программ, построенной по архитектуре «клиент-сервер», которая принимает вызовы со стороны **клиентской части**

сервер доставки, MDA, *pop-сервер*, *поп-сервер* – программа, работающая на сервере, где находится почтовый ящик абонента, и позволяющая ему забирать полученную электронную почту по протоколам POP или IMAP; часто его функции совмещены в одной программе с функциями сервера электронной почты (MTA)

сервер электронной почты, мейл-сервер, MTA – программа, осуществляющая прием и передачу сообщений электронной почты, поддерживающая почтовые ящики пользователей; работает на сервере, обычно обслуживает много пользователей одного или нескольких доменов электронной почты

серый IP-адрес – см. приватный IP-адрес

сетевая карта[52], сетевая плата, NIC (network interface card) – плата (устройство) компьютера, выполняющая функции взаимодействия с сетью по определенному интерфейсу; как правило, вставляется в слот расширения, иногда бывает интегрирована в материнскую плату; имеет один или несколько внешних разъемов для подключения сетевого кабеля либо антенну (для карт радиодоступа)

Сеть (с прописной буквы) – см. **Интернет**

сеть – см. **локальная вычислительная сеть**

сёрфер – человек, занимающийся просмотром веб-сайтов, как правило, увлеченный этим занятием сверх меры

сёрфинг, веб-сёрфинг – просмотр веб-страниц

си-ди – см. **компакт-диск**

сидиром, *сиди-ром* – см. CD-ROM

СИМ-карта – см. **SIM-карта**

симка – см. **SIM-карта**

система доменных имен – см. **DNS**

скво́ттинг – см. **киберсквоттинг**

скиминг (skimming) – вид мошенничества, заключающийся в «модернизации» чужого банкомата с целью считывания данных вставляемых карт и вводимых пин-кодов

скринсе́йвер, screensaver, заставка – программа, изменяющая содержимое экрана компьютера при неактивности пользователя в течение заданного времени; может содержать парольную защиту, то есть требовать авторизации перед отключением; в прежние времена скринсейвер предназначался для снижения нагрузки на люминофор электронно-лучевой трубки монитора, в настоящее время выполняет в основном декоративную функцию

[52] Термин упоминается в приказе Минсвязи №158 от 07.12.2006 и др. нормативных актах.

скриншóт (screenshot) – «снимок экрана», копия изображения на экране или в отдельном окне, каким его видит пользователь в момент съемки, полученный программными средствами и записанный в электронном виде в каком-либо графическом формате

скрипт-кидди – см. **script kiddie**

служба доменных имен – см. **DNS**

СМС – см. **короткое текстовое сообщение**

снифер, sniffer – программа (редко – программно-аппаратный комплекс) для сбора, просмотра и анализа всего проходящего трафика; является незаменимым инструментом для отладки и поиска неисправностей в сети, но также используется с вредоносными целями: для получения чужих паролей, организации ряда атак и т.п.

содержимое ОЗУ, дамп памяти – текущее состояние ОЗУ компьютера, снятое специальной программой и записанное на носитель долговременного хранения

сокс – см. socks-сервер

сорс-код – см. **исходный текст программы**

софт – см. **программное обеспечение**

спам (spam) – непрошенная массовая рекламная рассылка по электронной почте, реже по ICQ, SMS и др. системам электросвязи

спамер – человек, профессионально занимающийся рассылкой **спама** или сопутствующей деятельностью (сбор адресов, создание программ для рассылки, поддержание рекламируемых спамом ресурсов и т.п.)

субж, *сабж* – **поле «Subject»** сообщения электронной почты или сообщения в телеконференции

сырцы – см. **исходный текст программы**

телеконференции, newsgroups, группы новостей, *ньюсгруппы*, Usenet – система публикации и доставки сообщений на основе протокола NNTP [53, 54]

тема письма – **поле «Subject» в сообщении электронной почты**

техническое средство защиты авторских прав[53], ТСЗАП, DRM – любые технические устройства или их компоненты, контролирующие доступ к произведениям или объектам смежных прав, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором, обладателем смежных прав или иным обладателем исключительных прав, в отношении произведений или объектов смежных прав

трафик, сетевой трафик – (1) количество информации, переданное по цифровой линии связи, измеряется в битах или байтах; (2) реже термин используется в значении поток информации, т.е. количество информации, переданное в единицу времени, бит/с или байт/с; (3) содержимое передаваемых по сети фреймов, пакетов, датаграмм

[53] Термин определен в законе «Об авторском праве и смежных правах» (№72-ФЗ), ст. 48.1.

троянская программа, *троян*, троянец – вид вредоносной программы, которая, скрытно или маскируясь под безобидную программу, несанкционированно внедряется на компьютер пользователя для выполнения действий не в интересах и помимо воли пользователя (оператора)

установка программного обеспечения – см. инсталляция

учетная запись пользователя, аккаунт – регистрационная запись в компьютерной системе аутентификации, содержащая сведения о пользователе или ином субъекте информационного обмена, его аутентификационные данные (**логин** и пароль или хэш пароля), перечень полномочий и др.

файервол – см. **межсетевой экран**

файл (file) – именованная область диска или иного носителя компьютерной информации; имеет отдельно заголовок с именем и иными атрибутами и отдельно тело файла; является единицей хранения информации в файловой системе

файл подкачки, область подкачки, раздел подкачки – область на диске, являющаяся логическим продолжением **ОЗУ**, предназначенная для временного хранения содержимого ОЗУ, которое не умещается в реальной оперативной памяти

файловая система – структура записей на **НЖМД** или ином носителе информации, позволяющая эффективно организовать хранение данных; все данные хранятся в виде **файлов**

файлообменная сеть, пиринговая сеть, P2P-сеть – одноранговая или гибридная сеть компьютеров, оснащенных соответствующим ПО, которое позволяет распространять между участниками этой сети произвольные файлы, обеспечивая (а) надежность, (б) устойчивость, (в) высокую скорость обмена

фарминг – вид фишинга

фишинг (phishing) – вид сетевого мошенничества, основанный на выманивании у жертвы конфиденциальных персональных данных (данных банковской карты, паролей, личных идентификационных данных) с использованием подложных писем и/или подложных веб-сайтов, якобы исходящих от заслуживающих доверия инстанций (банков, провайдеров, государственных органов)

флоп – см. **дискета**

флоппи-диск – см. **дискета**

фрикер – специалист по преодолению защиты аппаратных электронных устройств

фронт-офис (front-office) – часть информационной системы или интерфейса информационной системы предприятия, предназначенная для клиентов предприятия, партнеров, иных внешних пользователей; термин используется при сопоставлении с бэк-офисом

хаб – см. **концентратор**

хак – см. **несанкционированный досту**п

хакер – (1) компьютерный специалист очень высокой квалификации; (2) злоумышленник, осуществляющий несанкционированный доступ к компьютерной информации, обычно через сеть

циска – коммуникационное устройство производства фирмы «Cisco Systems», маршрутизатор или коммутатор; иногда в нарицательном смысле – любой **маршрутизатор** или **коммутатор** (аналогично тому, как любой копировальный аппарат называют ксероксом)

ЦПУ – см. **процессор**

чайник – малоквалифицированный пользователь ЭВМ

чарджбэк – см. возврат платежа

читинг (cheating), чит (cheat) – обман, обход и нарушение установленных правил игры в компьютерных играх; может быть вполне приемлемым (если игрок играет против компьютера), неприемлемым (если играет против других игроков) и даже незаконным (если игра идет на деньги)

ша́ра – сетевой ресурс, доступный многим пользователям

шарить, *расшарить* (от share) – делать сетевой ресурс доступным другим пользователям

эквайрер – кредитная организация, осуществляющая эквайринг

эквайринг – деятельность кредитной организации, включающая в себя осуществление расчетов с предприятиями торговли (услуг) по операциям, совершаемым с использованием банковских карт, и осуществление операций по выдаче наличных денежных средств держателям банковских карт, не являющимся клиентами данной кредитной организации

электронная почта – система обмена сообщениями через сеть, работающая по протоколу SMTP, а также сами эти сообщения

эмулятор – программа или часть программы, которая эмитирует (эмулирует) для других программ работу аппаратного устройства или удаленного узла, сервера, компонента; например, программа-эмулятор может заменять отсутствующий аппаратный ключ защиты, являясь при этом средством обхода ТСЗАП

[54] Термин введен в гл. 28 УК РФ – «Преступления в сфере компьютерной информации».

Н.Н. Федотов

Форензика –компьютерная криминалистика

Москва, «Юридический Мир», 2007. – 360 стр.

Сдано в набор 00.08.2007, подписано в печать 00.00.2007.
Формат 60x90/16.
Печать офсетная. Печ. л. 22,5.
Тираж 3000 экз.

Издательство «Юридический Мир».
105064 Москва, Земляной Вал, д. 38-40.
www.legalworld.ru